ENHANCE YOUR IT STRATEGY

DIGITAL LEADERS

2016/2017



Part 2: SECURITY

bcs The Chartered Institute for IT



Image: iStock.com/maxkatakov

TIPS FOR SECURITY SUCCESS

Dawn James MBCS, an Information Security Project Manager, shares her 'Top 5' critical success factors for cyber security education based on years working on cyber security education programmes in both small and large organisations.

The developments in technology such as cloud computing and apps, tablets and smartphones have now totally transformed the way people work. However, the number of high profile and very serious data breaches appear to be increasing.

The ransomware attack in the German hospitals case (1) resulted from an employee accidentally opening an email containing the malware, which consequently encrypted the data of servers and computers, rendering the data inaccessible to the devices that needed it.

This is the latest victim of an increasing trend where hackers use ransomware (2) to encrypt the organisation's data, and then demand money to decrypt the data.

Statistics from the 2015 Information Security Breaches Survey(3):

- 75 per cent of large organisations and 31 per cent of small business have suffered a staff related security breach within the last year – up from 58 per cent and 22 per cent respectively from a year ago
- 50 per cent of the worst breaches in the year were caused by inadvertent human error – an increase of 31 per cent from a year ago
- 72 per cent of large organisations and 63 per cent of small businesses provide ongoing security awareness training for their staff – up from 68 per cent and 54 per cent respectively from a year ago
- Cost (average) to a large organisation of a worst-case security breach was £1.46 million to £3.14 million – up from £600K to £1.1.5 million from a year ago
- Cost (average) to a small business of a worst-case security breach was £75K to £311K from last year – up from £65K to £115 K from a year ago.

Although security awareness training has increased, so has staff-related security breaches, half of them attributed to human error.

Cyber security education still has some way to go.

Cyber security versus information security

The word 'cyber' is now a much used term. However, cyber security education should also include the protection of all forms of information, for example, printed, stored on removable media or portable computers such as tablets and smartphones.

Recall the HMRC data breach(4) way back in 2007, where two discs containing child benefit data went missing in the post, resulting in the resignation of the chairman of HMRC.

Awareness, training, education

Raising awareness is a good start. However, users can be aware of cyber security risks, but unaware of how to recognise and handle a potential threat. The German hospitals breach may have been prevented by a reminder to employees regarding not opening suspicious email.

Regular training, reminders and ways of measuring the effectiveness of the training are also required, for example, conducting post-training tests and questionnaires to reinforce user learning.

It is useful to have a multi-discipline team, led by a well-trained cyber security team – not just the IT department. Human resources (HR), legal, internal audit, department heads and business managers, and the internal media and communication team if available, need to input into the project.

The 'Top 5' critical success factors

1. Senior management support

When senior management and board members are seen to be giving visible and active support, I have found that users are far more likely to respond and participate in cybersecurity initiatives.

Users can be aware of cyber security risks, but unaware of how to recognise and handle a potential threat.

Getting senior management buy-in is by no means an easy task but, in my experience, it helps to demonstrate, in monetary terms, how much a breach has or will cost the organisation, in addition to the 'scary' cyber breaches headlines. Otherwise, cyber security is simple ignored or treated as just a 'tick-box' exercise to be completed as quickly as possible to satisfy internal audit and compliance.

This is appears to be supported by the PwC 2015 Information Security Breaches Survey, which states that '28 per cent of the worst security breaches were caused partly by senior management giving insufficient priority on security', up from 7 per cent a year ago.

2. Cyber security policy

A brief, understandable and readily accessible cyber and information security policy should form the foundation of the cyber security education programme.

The policy set should also include acceptable use of email, software and computers, password security, incident response, virus prevention, social media, home and mobile working, and the use of personal devices for work purposes where permitted.

Policies should also make clear the responsibilities of employees (consultants, contractors, temps), and the consequences for non-compliance. The input of the HR department and the legal department should be useful.

3. Good quality training materials

The quality of the training materials is very important when getting the message across. Judging by most users' reactions, nothing is worse than poor quality training materials and this tends to users ignoring the message.

There are many tools available and vendors offering cybersecurity training. Any tool selected should be scalable, easy to use, customise and maintain, and meet the organisations' requirements.

The ability to track whether users have completed the training, any areas of security they may have difficulties with, and follow-up action is also very important.

Internal branding of the training materials makes cyber security instantly recognisable to users, and is also useful for getting the message across.

4. Face-to-face delivery

Classroom style training appears to be the most effective way for cybersecurity awareness and training. Participants tend to ask questions if they don't understand a particular subject, and the session is more interactive than purely computer-based training. Users also appreciate the training more when it is fresh, engaging, topical and relevant to their work.

I have had many discussions with users about email use, on-line scams, secure shredding, not necessarily all work-related. This also gave me the opportunity to explain the relevance of important legislation such as the Data Protection Act(5) , Computer Misuse Act(6), which most users are not aware of in my experience.

This approach depends on the size of the organisation, the number of staff in the delivery team and the budget allocated to the activity. This may not be feasible for larger organisations.

Note that ISO 27001(7), the international standard for information security, states that training should be 'appropriate', 'regular', and 'relevant'.

5. Culture of openness

In an open, honest culture, employees are far more likely to engage and participate with cybersecurity initiatives, than if a 'blame culture' dominates. This is particularly important when reporting incidents; users may be educated and aware of cyber security, but can still make mistakes that may consequently put the organisation's data at risk.

To conclude, when it comes to the 'cyber war', your employees are the 'frontline'. Time, money, and resources should be spent on educating your most valuable asset of all – the people.

Further reading

"Ransomware holds data hostage in two German hospitals" - SC Magazine, Rene Millman, 29 February 2016 [accessed 11 April 2016]

SANS website Newsletters: "US Federal Agencies and Ransomware (March 30, 2016)"; **www.sans.org** [accessed 11 April 2016]

PwC 2015 Information Security Breaches Survey, Executive Summary, PDF [accessed 11 April 2016]

BBC News "Data lost by Revenue and Customs", 21 November 2007; [accessed 11 April 2016]

Data Protection Act 1998: **www.legislation.gov.uk/ukpga/1998/29/contents** [accessed 11 April 2016]

Computer Misuse Act 1990: **www.legislation.gov.uk/ukpga/1990/18/contents** [accessed 11 April 2016]

BSI Group factsheet: "Need to protect your information?" [accessed 11 April 2016]



Image: iStock.com/Valeriy Kachaev

David Bird MBCS CITP discusses satellite system vulnerabilities, which could be the next battlefront for cyber warfare.

The communications transformation fuelled by the internet has been immensely progressive and it is well known that this distributed network has provided the backbone of the Information Age. There is, however, a little known fact that satellites have played an important role in extending global connectivity and providing heterogeneous internetwork resilience – something that we perhaps take for granted today. Unfortunately recent events have identified a number of weaknesses that were in fact predicted as far back as 2001 within a United States Senate report.

It was surmised then that satellite system vulnerabilities could be exploited and the associated risks should be combatted through: the implementation of secure data links; protective measures at the satellite ground stations; and/or secure approaches that enhance availability.

Unfortunately, under the right conditions, and through implementation oversights relating to the first two, hackers can use such deficiencies as cyberattack vectors. These could provide an opportunity for hackers to cause a negative physical impact pertaining to the third.

Important technologies

Approximately 52 per cent of satellites are located in low Earth orbit (LEO), which is a geocentric orbit up to 1,243 miles above the surface; this is ideal for photographic satellites such as Cubesats and some US National Oceanic and Atmospheric Administration (NOAA) satellites, as well as real-time voice telecommunications satellites such as Iridium.

The most well-known orbit is the geosynchronous Earth orbit (GEO) in which 41 per cent of satellites reside at 22,236 miles altitude; most satellite communications (SATCOM) spacecraft reside in particularly desirable, cluttered and highly regulated orbital slots and radio frequency (RF) spectrum allocations issued by the International Telecommunications Union.

The medium Earth orbit (MEO) is the space for the remaining 7 per cent such as Global Positioning System satellites, which are in an intermediate circular orbit at an altitude of 12,500 miles . The graveyard orbit, in high Earth orbit, is where higher altitude satellites are despatched at the end of their usable life. LEO vehicular orbits tend to decay backward toward the Earth where spacecraft mostly burn up on re-entry through the Earth's atmosphere.

Traditionally satellites have been used to relay narrowband telecommunications under 1GHz encompassing L band in LEO.

This has extended into wideband ranging from below 4GHz to 40GHz S, C, X, K series bands into high capacity broadband in Ka; high capacity is now pushing the envelope through Q, V and W frequency ranges between 30 to 75GHz and 75 to 110GHz retrospectively. The achievable data-rate is dependent on the orbit and SATCOM has progressed immensely enabling, at best, a honeycomb of multiple beams to provide high-throughput data services over a large area of the Earth.

The increase in data-rates is enormous; expanding from a measly 480kbps at the top of the L-band to 130Gbps, achievable through ViaSat1 Ka band in GEO, upwards to an expected 350Gbps in the Ka band with ViaSat2 by late 2016. MEO is fast becoming more necessary for SATCOM as it offers less delay than GEO; the latter usually has a round trip latency of around 500ms where the former is now known as the 'fibre optic orbit', achieving broadband throughout at around 100ms.

As a consequence a SATCOM programme called the 'Other 3 Billion' (O3B) provides MEO SATCOM mobile and internet coverage to developing nations from a 5,000 mile high orbit.

Hypothetically satellites can be susceptible to RF jamming.

Vulnerabilities and cyber threats

Space is a harsh dominion where satellites are constantly bombarded by space weather and their uplinks/downlinks are affected by atmospheric attenuation and depending on the frequency band global weather interference. Notwithstanding these issues, hypothetically satellites can be susceptible to RF jamming.

In addition congested orbits increase the probability of space collisions, which could knock-out satellites. Notably in 2014 the International Space Station had to be manoeuvred three times to avoid prolific space debris. This risk has been reinforced and epitomised by the 2007 Chinese anti-satellite kinetic weapon test that created a shroud of unnecessary space debris and an ensuing international political outcry; worryingly it is claimed that China may soon have the capability to destroy every satellite in orbit.

Historically the probability of mechanical satellite failure is greater than electrical – although platform computer malfunctions cannot be discounted. There is now evidence of cyber attack attempts that were conducted against National Aeronautics and Space Administration (NASA) low-Earth environmental monitoring satellites between 2007 and 2008; whereby the telemetry, tracking and command link via an Arctic ground station was used as the conduit for the attack.

In 2014, it became apparent that unpatched software, poor configuration or misconfiguration were evident on satellites being built as part of NOAA's Joint Polar Satellite System space segment – providing an attack surface onboard the platforms themselves. Newsworthy reports in the same year alleged backdoors and insecure protocol usage in commercial satellite terminals and patching was advised to alleviate vulnerabilities in some user segment equipment.

The lack of encryption on data channels has been diagnosed as a flaw for an established commercial satellite-borne tracking and monitoring system that could enable hackers to manipulate, spoof or affect the reliability of data being transmitted .

In 2013, it appears that a NOAA contractor's laptop was infected with malware and was subsequently used by a remote attacker to exfiltrate data from a national environmental satellite, data, and information service system onwards to a suspicious external IP address .

In addition the well-publicised cyber-attack of late 2014 against NOAA's four websites caused an unscheduled outage of their networks; the effect being the cessation of their customer facing global data services supplied from their LEO and GEO constellations - creating a denial of service.

Fatal consequences?

Satellites are inevitably becoming more crucial than ever in our digital world. Whether SATCOM orientated, Earth facing scientific, meteorological, photographic or astronomy focused; they are all supplying data and services for the 21st century consumer. The positive outcome of satellite technology, for instance, has enabled third generation cellular infra-structure providers to use SATCOM as backhaul links over many years. This approach is liable to continue to provide supporting data service trunks for increasingly important

fourth generation mobile technology and beyond.

It is clear that oversights across the space industry are potentially quite serious and could affect the confidentiality, integrity and availability of some satellites and satellite services – as predicted in the 2001 Senate report. Only recently the hacker group AnonSec demonstrated intent by trying to crash a NASA drone; their modus operandi was to alter the flight plan after taking control of ground segment servers, but only after having been allegedly resident in NASA networks for some months.

It is entirely feasible that the Kessler Syndrome, usually linked to the consequences of the build-up of space junk, could be instigated and accelerated by hackers. Hackers may have the guile to irresponsibly take control of a vulnerable satellite and naively cause accidental or deliberate collisions in a congested orbit.

Such an act is not beyond reason and could be the catalyst for a catastrophic self-sustaining orbital collision, conceivably wiping out some of mankind's satellite constellations in the process!

On the weight of this evidence the cyber security of the space segment, the requisite user segment, and especially the ground segment command and control systems should be made justifiably more robust moving forward.

References

1 R.Dacey, 2001, Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed, GAO, Diane Publishing, pp20, 32-33.

2 D.Minoli, 2015, Innovtions in Satellite Communication and Satellite Technology, Wiley, pp2

3 E.Gunduzhan et al, 2015, Narrowband Satellite Communications: Challenges and Emerging Solutions, Johns Hopkins APL Technical Digest, Volume 33, Number 1.

4 J.Yates, 2015, Satellite Communications presentation, IET.

5 J.Amos, 2010, O3b 'fibre in the sky' project wins financial backing, **www.bbc.co.uk/news/science-environment-11847708**

6 C.Riedl, 2014, Internet at fibre optic speeds, **www.munichre.com/touch/space/en/solutioncompetence/O3B/Overview/index.html**

7 C.Moskowitz, 2011, Space Junk Problem Is More Threatening Than Ever, Report Warns, **www.space.com/12801-space-junk-threat-orbital-debris-report.html**

8 Horizon, 2015, The a Trouble With Space Junk, BBC

9 L. David, 2007, China's Anti-Satellite Test: Worrisome Debris Cloud Circles Earth, **www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html**

10 K.Zachary, 2015, China's Next Super Weapon Revealed: Satellite Destroyers, **www.nationalinterest.org/blog/the-buzz/chinas-next-superweapon-revealed-satellite-destroyers-12640**

11 J.Wolf, 2011, China key suspect in U.S. satellite hacks, **www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028**

12 A.Sternstein, 2014, Pentagon Satellite Maker Ignoring 'Thousands' of Major Cyber Vulnerabilities, **https://cdn.defenseone.com/defenseone/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.defenseone.com%2Ftechnology%2F2014%2F08%2Fpentagon-satellite-maker-ignoring-thousands-major-cyber-vulnerabilities%2F92477%2F**

13 K.Jackson, 2014, No Fixes in Sight for Satellite Terminal Flaws, **www.darkreading.com/vulnerabilities---threats/advanced-threats/no-fixes-in-sight-for-satellite-terminal-flaws/d/d-id/1297882**

14 BBC, 2015, Globalstar tracking system 'open to attack', **www.bbc.co.uk/news/technology-33731185**

15 A.Sternstein, 2014, Hacker Breached NOAA Satellite Data From Contractor's PC, **www.nextgov.com/cybersecurity/2014/07/hacker-breached-noaa-satellite-data-contractors-pc/89771/**

16 M.Gruss, 2015, NOAA Admits to Cyberattack on Satellite Data Networks, **http://spacenews.com/42561noaa-admits-to-cyberattack-on-satellite-data-networks/**

17 S.Peters, 2014, NOAA Blames China In Hack, Breaks Disclosure Rules, **http://www.darkreading.com/noaa-blames-china-in-hack-breaks-disclosure-rules/d/d-id/1317460**

18 SatCom WG, 2014, The role of satellites in 5G, Networld2020.

19 iDirect, 2013, Extending 3G and 4G Coverage to Remote and Rural Areas Solving the Backhaul Conundrum.

20M.Thalen, 2016, Hackers Allegedly Hijack Drone After Massive Breach at NASA, **www.infowars.com/hackers-allegedly-hijack-drone-after-massive-breach-at-nasa**

21Dr H.Lewis, 2015, Trouble in orbit: the growing problem of space junk, **http://www.bbc.co.uk/news/science-environment-33782943**



Image: iStock.com/RyanKing999

AUDITING CLOUD: SECURITY VS AGILITY

Cloud computing still involves many risks concerning security, integrity and network dependency. Reza Alavi, from BCS IRMA Academic Relations, discusses the security issues of moving to the cloud.

Moving on-premises data centre architectures onto the cloud is what organisations are doing in order to deliver additional value and to increase business agility. But businesses encounter serious risks from security incidents. The threats to assets, application performance and critical business data, creates further risks such as availability, authentication and virtual exploit risks through virtualisation.

The vast majority of businesses have already adopted cloud computing. Information assets and data have drifted away from the complexity of being hosted on premises with a dedicated physical server and local client applications to the cloud and this trend is growing in momentum.

Constructing IT infrastructure in the cloud is a very different process from structuring a traditional network. Service level agreements (SLA) have become more concerned about connectivity and service availability. Therefore, organisations transformed and improved their service levels, reliability, return on IT investment and security, all by using cloud services.

Virtualisation platforms for public, private or shared cloud services, are now available widely. Service providers like Amazon Web Services and Microsoft Azure, provide all sorts of cloud solutions, from data storage to information processing services and applications.

Increased ability and agility

One of the main opportunities for businesses in moving to the cloud is the ability to work with a wider range of vendors providing highly specialised solutions. There are many issues which heavily impact the choice of cloud vendors. The rate of growth, the ever changing and forthcoming business and organisational challenges, the compliance ecosystem, and the technology landscape all are important matters for businesses.

These issues, as well as agile and ad hoc business, and organisational and technological challenges, can all create security and auditing difficulties for many businesses.

The cloud facilitates low-cost agile innovation, but at the same time brings its own challenges, including security and auditability concerns. Cloud enables a company or entrepreneur to create a new product or service on the internet without having access to huge capital investment. This includes servers, computers and full information system capability. Nowadays, any business idea can go live in a very short space of time. However, this requires the availability of the security products. This concerns anything related to data. Data is the most worrying security issue in the cloud environment. It requires encryption and adequate management of data. Therefore, auditing the cloud has become a massive headache for organisations.

The auditing process is essentially an assurance function that depends on the type of audit. It requires the auditor to systematically examine proof of compliance to established criteria. Understanding of organisational functions allows the establishment of the scope of the auditing process by identifying and mapping IT infrastructure to those functions to provide the best suited controls for them.

The very same requirements apply to the cloud. However, as business functions shift into a cloud environment, new risks to systems emerge. This is as the result of differences between cloud architectures and systems hosted by traditional IT infrastructure. Cloud architecture introduces some very likely changes that will impose modifications to the auditing process and scope.

Thorough testing

Moving an IT function to the cloud does not mean that the controls which protected that function in the internal organisational infrastructure will be moved to the cloud. This function which will be hosted by the cloud vendor. For example, many organisations do not run encryption of data or strong authentication and access controls on their premises. Instead, they rely on the existing security and controls of their internal systems.

The lack of access controls and authentication will compromise the very same data when it moves to the cloud as the same process has not been considered over there. Many in-house developed applications have not been tested for common internet vulnerabilities as they are heavily relying on the internal security and controls of organisations. Therefore, they may be vulnerable to a variety of breaches, scripting, hacking and worms. These applications must be tested carefully and thoroughly to guarantee access controls and authentication process.

Identity management would be another area of concern as in internal and local networks this can be run from a single centrally controlled service model such as active directory Kerberos and OpenLDAP of Linux or Red Hat Directory Server. This may introduce new risks due to the complexity if they do not test to the auditor's satisfaction.

Another important issue in the process of auditing the cloud is about endpoint security. Ordinary and traditional networks expect to have firewalls that allow them to provide endpoint security despite a workstation turning off the firewall services as they assume protection within organisational infrastructure, which can be compromised in the cloud environment.

> One of the main opportunities for businesses in moving to the cloud is the ability to work with a wider range of vendors providing highly specialised solutions.

Finally, the cloud servers are under maintenance and they get patched by the cloud vendors. Auditing the cloud should confirm and reaffirm that vendors maintain and patch the servers to address new risks. Organisations should work collaboratively and narrowly with the cloud vendors in that direction.

New changes bring new challenges

Cloud services, regardless of their type - hybrid, public, or private - bring crucial changes to the network and IT services in respect to audit scope and process. Organisations can only address this challenge by a close and collaborative communication with the cloud vendors. There are some distinctively important control areas in the cloud such as control access, authorisation and trusted control frameworks, which differentiate the

auditing process of the cloud to the internal infrastructure. This should be considered by auditors.

Cloud hosted services, data, infrastructure and applications create new challenges for auditors as data privacy should consider international laws as data moves from one location to the other one in various geographical positions.

As effective audits require appropriate scope and controls, this will be unique to every system, therefore, auditors should study cloud resolutions cautiously. Audit requires a clear solution to the conflict of interests and evidently assert findings and qualified opinions-based evidence and documentation. This is quite similar to the auditing process of traditional infrastructure.

The main difference in audit comes from the various deployment models, including private, public or hybrid, as well as service model. The service model includes software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).

The main variances are in the public and hybrid models because they rely greatly on contracts and complex SLAs and compliance to those agreements. Therefore, planning and implementing an audit process must consider that the organisational network will use the internet, so, the controls and other relevant features should be appropriate to these conditions.

Achieving a balance

Functionality of organisations is dependant, quite profoundly, on IT services. This reliance moved on at an exponential rate to the cloud platform and that introduced a number of risks to IT and, consequently, to organisations.

Cloud provided a serious and fundamental change in the way business models work. Legal, reputational and financial costs are the risks of the failures of the system and it is very hard to be compensated if cloud deployment fails.

Whilst cloud solution create economic advantages, the risks for failure are severe. IT risks create business risks and a balance is required. So, the auditors must be able to remodel their approaches to new technology and novel methods.

Data is processed in order to make an accurate risk and audit assessment. Auditors should modify and familiarise themselves with new challenges, vulnerabilities and threats in the cloud environment. The new cloud control models that introduced by the Cloud Security Alliance, NIST, and ISACA and should be learnt and exercised by auditors. This also concerns those organisations who are required to constantly check up on the most current guidance associated with the above cloud-related frameworks or standards. Organisations can achieve balance between business risk and opportunity if they invest in an appropriate, effective and adequate internal audit of their cloud deployment.

Further reading

Alavi, R., Islam, S. and Mouratidis, H., 2015. Human Factors of Social Engineering Attacks (SEAs) in Hybrid Cloud Environment: Threats and Risks. In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security (pp. 50-56). Springer International Publishing.

Pearson, S.,Yee, G., 2013. Privacy and Security for Cloud Computing. Springer, London.

Hogan, M. & Sokol, A., 2011. NIST Cloud Computing Standards Roadmap. In: Commerce, U. D. O. (ed.). National Institute of Standards and Technology (NIST). [Cited January 2016]. **www.nist.gov/customcf/get_pdf.cfm?pub_id=909024**.

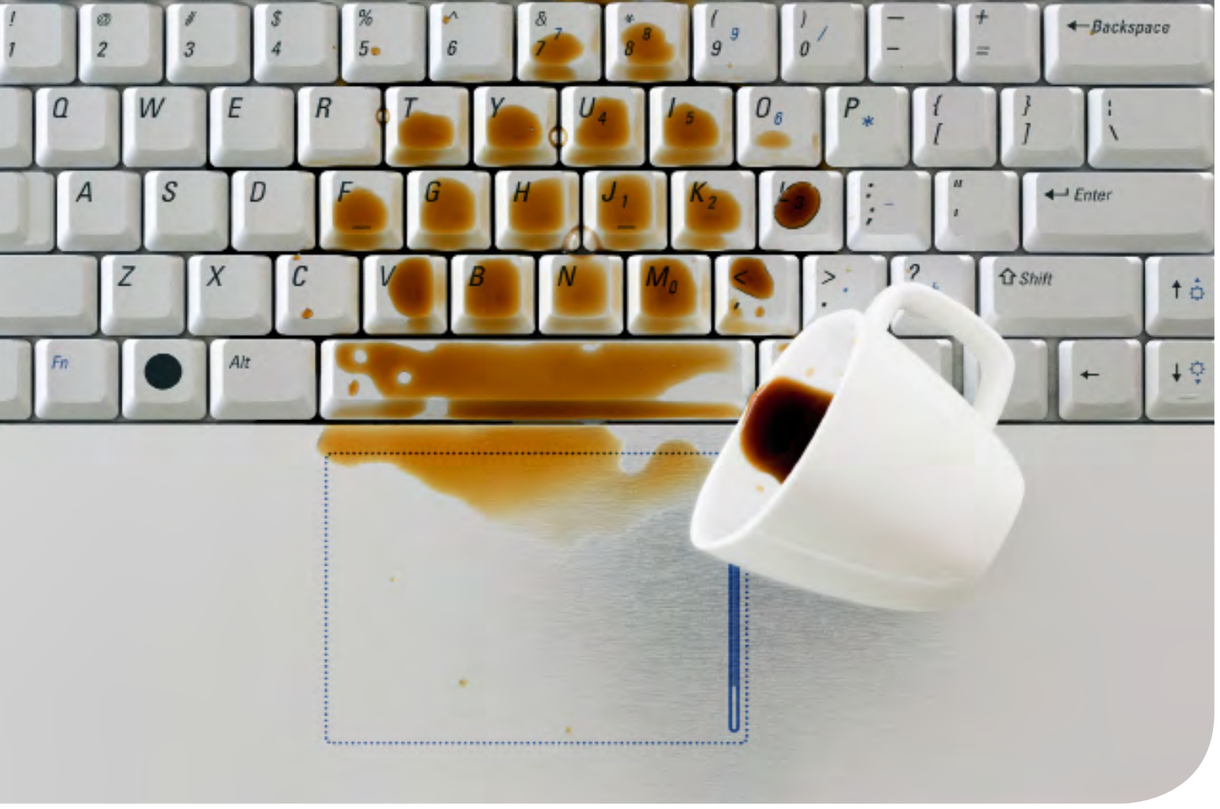


Image: iStock.com/Paket

PREVENTING SPILLS

Juliet Flavell, MBCS, IT Manager and Information Risk Management and Assurance committee member, discusses mobile device management, and data leakage in particular.

Two major concerns have been occupying IT professionals during recent years in relation to the integrity, availability and confidentiality of information on their systems. First, the ubiquitous, but invisible, subtly developing menace of cyber threats.

This now also encompasses old-fashioned con tricks and manipulation of human targets. Defending against these social engineering attacks is interestingly often seen to be the responsibility of the IT department, although well outside the traditional scope of the IT role. Second, the shifting boundaries of the network and the ongoing challenge of preventing data leakage, whether deliberate or accidental.

Managing mobile

Mobile device management (MDM) is a tool supporting an organised approach to the problem of data leakage through devices. It is a centrally managed software tool providing a simple way to get business-critical information, like emails and documents, securely onto mobile devices and to help safeguard that information. The offering has developed since my firm first started using it and has now extended to manage laptops, PCs and printers, although we currently use it only for mobile phones and tablets.

The driver for our project at an SME law firm was a commercial decision to provide all the lawyers with corporate-owned mobile devices. This was partly motivated by the need to minimise 'down time' while waiting at court, often for unpredictable lengths of time. Lawyers charge by their time and are required to be transparent about this so every minute counts. Other requirements were the ability to check emails away from the office and the safeguarding of privacy by stopping lawyers having to give out their personal mobile numbers to clients.

Prior to this we had given some lawyers access to work emails on an ad hoc basis using BYOD. This presented problems around support due to platform diversity. Ease of support is crucial in small organisations so standardising on one hardware platform was a no-brainer. By providing them with a corporate-owned phone, we had more control over client's personal data and the lawyers had control over their own personal data.

An on-site installation of the MDM would have been an option had we been a larger organisation, but for us the cloud platform with its web-based console was the right solution. Installation and testing were straightforward. Our mobile phones are companion devices providing functionality being introduced for the first time and the devices are cheap enough to justify a dedicated spare for testing.

Support and security

MDM works by the phone's owner giving control of the phone over to the MDM administrator (IT). For the users, this is barely noticeable. From a support perspective the console is straightforward, but behind the scenes it interfaces with the phone's operating system. Security settings are applied in the form of profiles. We enforce a complex passcode and the devices lock quickly when idle. There are restrictions on apps, which may be installed, and they must be chosen from an app catalogue on the device. Apps incidentally can be configured not to back up their data, and to uninstall automatically on unenrolment. During the first wave of testing, we removed the native camera app, assuming it to be a redundant feature, only for it to emerge that lawyers often legitimately photograph court orders. Tweaking and remotely redeploying the profile quickly restored this functionality.

It's also possible to integrate with Active Directory. There is a secure container for distributing documents to the lawyers. As the blurb says, this 'containerises corporate content and keeps it secure with FIPS-140 compliant 256-bit SSL encryption, location and time-based access, and printing restrictions'. Restrictions can further be configured for web browsing, and continuous monitoring keeps devices compliant.

If a device is compromised, non-compliant or the user leaves the company we can automatically disable access and wipe content. In terms of corporate email, administrators can configure policies to prevent copy/paste/forwarding and disable access. We can further stipulate that attachments be opened, viewed and stored in the secure container.

Alerts can be configured for continuous compliance monitoring and reports scheduled, for example to list installed apps. This enabled us to see that one lawyer had added a personal Apple ID to their iPad and used it to install apps for their young child to use – potentially an insider threat, however innocent!

We enrolled all the devices manually (although it can be self-service) and combined the handover with a written set of 'golden rules' around best practice and points to note. In small organisations, an uncomplicated and frequently-reviewed set of rules around information protection is essential. We don't have as much time or money as larger organisations to dedicate to cybersecurity therefore a set of often-reinforced pragmatic procedures around the protection of information is key.

Controlling a breach

How would MDM help us detect and control a potential breach? It gives visibility over devices. If an employee fails to return their device after leaving, we could remotely lock the device, reset the passcode, change their email password and make any corporate data such as emails, calendar, secure content, permitted apps and their associated content simply evaporate from the device.

Location services are enabled by default so we can, in theory, track where a device is at any time, although in practice this can be somewhat patchy in its reporting. It's also possible to make a message appear on the device's home screen, even when locked. We used both of these features to good effect when an iPad was lost and had reported its last location as the Blackwall Tunnel late the previous night. Thanks to our 'this device has been reported lost or stolen' message appearing on the screen with a contact phone number, the device was returned safely to us by a very decent cabbie (who was naturally rewarded with a very decent tip)! The MDM console even shows the percentage of battery life remaining – a factor in deciding whether to remote wipe or not.

The threat of people working under pressure to very short deadlines using workarounds bypassing security measures in order to make life easier, is all too evident. Lawyers have become exponentially busy with the requirement to record all their chargeable time down to the last minute so their costs are transparent to clients. For IT, finding a balance between keeping risk at acceptable levels, while not making life overly restrictive for staff, forcing them into using workarounds, is a tough nut to crack. MDM has helped with this.

It's impossible in my view to guarantee that there is not some malware that can circumvent some of the controls our MDM puts in place, and you should not assume that there isn't. Our practical set of 'golden rules', and accompanying usage policy, are not a technology solution, but are nevertheless essential and leave us with an acceptable level of risk. Certainly the software pays for itself in money saved through greater efficiency. But these days a multi-layered approach is needed – part technology and part human behaviour.

MDM is a good techology solution. It gives you a great deal of visibility over devices in use and a strong tool for protecting data on those which have been lost or stolen.

Finding a balance between keeping risk at acceptable levels, while not making life overly restrictive for staff, forcing them into using workarounds, is a tough nut to crack.

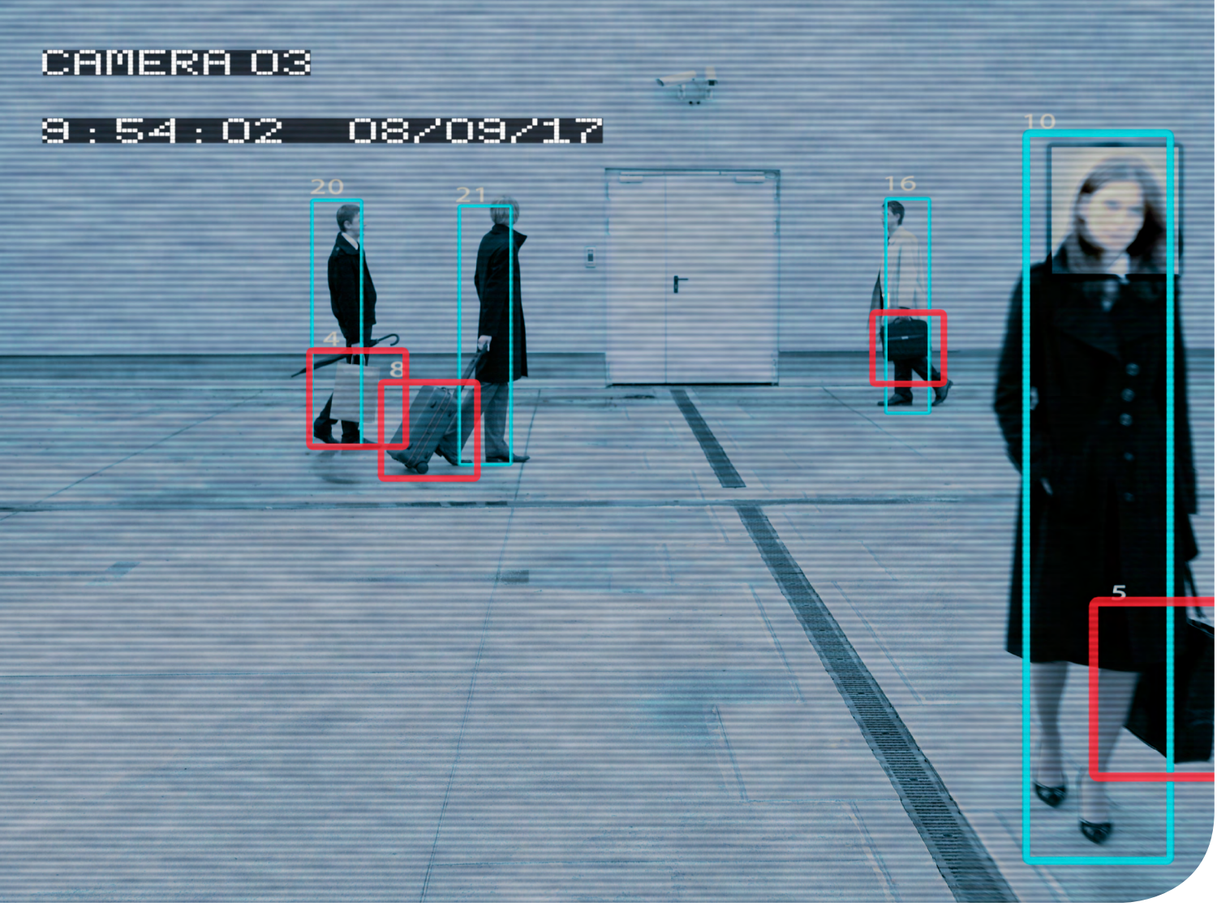


Image: iStock.com/ER_Creative

YOUR LIFE IS ~~ON THE LINE~~ ONLINE!

Vijayaratnam Ganeshkumar FBCS, Maninablacksuit.com, considers the brave new world that we find ourselves in, where having an open, trusting society also comes with a darker caveat, that of nations guilty of higher levels of surveillance than most of us are comfortable with...

Today I took the public transport to the office. On my way, I had breakfast at a coffee shop and until I reached the office, I met several individuals: a bus driver, the person seated next to me, and a waiter.

What would have happened if the bus driver had kidnaped me and asked for a ransom or the person sat next to me on the bus had threatened me and tried to steal from me or had tried to kill me?

On the other hand, what if the café person had poisoned my food? Society does not work like this, society works on trust. The nature of society requires some measure of trust and humans are a trusting species.

Trust is a complicated concept, and this word is overloaded with many meanings. All complex ecosystems require cooperation. This is true for biological ecosystems, social systems and sociotechnical systems. Also, in any cooperative system, there also exists an alternative parasitical strategy. A tapeworm in your digestive tract, thieves in a market, spammers on e-mail, and people who refuse to pay their taxes.

These parasites can only survive if they are not too successful. That is, if their number gets too large or too powerful, the underlying system collapses. If there are too many tapeworms in your digestive tract, you die and they die. If there are too many thieves in a market, no one will visit the market anymore and the thieves will starve. If too many people stop paying their taxes, you get economic collapse.

If everyone decides to act in an antisocial way society soon collapses. Most of us recognise this; that it is not in our long-term, best interest to act in our short-term self-interest. Sadly, not everyone does and that's why we need mechanisms to induce trust and why we need security.

Nowadays we hear lots of terrorising news: cyber terrorism, cyber war and cybercrime. Cyber war; it is not a military action; there are no guns, bombs or people dying, but we love to use the word 'war' even where there is no war. The war on terror, war on drugs and war on crime. Although we hate using the word 'war' when there is an actual war! We will say anything else other than war. In a real war, you know who is attacking and why they are attacking. However, in the case of cyberwar, you do not know when, why and who is attacking. To control cyber threats, we need lawful surveillance. Once again 'lawful' is a convoluted word.

The number 3000

This is the number of times a single citizen is caught on camera, within a 24 hour period, in the UK, by some of the 5 million CCTV cameras we have here, in the most heavily surveillanced country in the world.

Have you ever questioned yourself: 'How much does Google really know about me?. It probably knows more about you than your partner! We have lost our privacy.

What does privacy mean and why is it important?

Privacy is the right to be left alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and then used.

Privacy and security... isn't it the same thing? Not really, but they are 'kissing cousins'. Security and privacy are not opposite ends of a seesaw - you don't have to accept less of one to get more of the other.

Data privacy is focused on the use and governance of personal data. On the other hand, security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit.

When Edward Snowden leaked massive troves of information about the National Security Agency's collection of electronic data, he started a debate over the tradeoffs between security and privacy. Unfortunately, the security vs privacy debate is largely over. As cyber-technologies pervaded our daily lives, we surrendered privacy, usually voluntarily.

Consequently, framing the decisions before us as a contest between privacy and security is misguided; privacy died with the information age.

Are we surrendering our privacy for technology?

The answer is: Yes. Information and communication technologies make life better. They improved productivity, efficiency and economic growth. However, these benefits come at a price. Simply look at your cell phone. This cute, sleek, incredibly powerful tool has become so central to our lives that we take it for granted. It seems perfectly normal to pull this device out of your pocket, no matter where you are on the planet, and use it to talk to someone else, no matter where the person is on the planet. You are making an implicit bargain with the carrier: 'I want to make and receive mobile calls; in exchange, I allow this company to know where I am at all times.' A cellphone can't work unless the cell phone companies know where you are, which means they keep you under their surveillance.

Your cell phone tracks where you live and where you work. It tracks where you like to spend your weekends and evenings. It tracks how often you go to church (and which church), how much time you spend in a bar, and whether you speed when you drive. It tracks—since it knows about all the other phones in your area—who you spend your days with, who you meet for lunch, and who you sleep with.

Explaining in simple terms: in a public place, whatever the place you think of, an unknown person approaches you and asks for your personal details (it can be your name, age or mobile). Will you give them that information?

Nearly 99.9 per cent will say 'No', because the person is unknown to you and why should you give it to an unknown person? When the enemy is a known threat, we defend ourselves, if unknown, we often expose more than the enemy actually wants; this is what happens in this information age.

Have you ever questioned yourself: 'How much does Google really know about me?' It probably knows more about you than your partner! We have lost our privacy.

How many of you have social network accounts (Facebook, LinkedIn)? Do you know how much of your personal details are being uncovered? On the other hand, social networking plays a bigger role in our lives. We need this, to be connected with our friends, to businesses for marketing and for exposure. However,

technology advancement comes with a price, and we have to bear it.

In 2013 Edward Snowden, the whistle blower, sacrificed his freedom and exposed NSA's secret surveillance. The whole world was shocked that we are under surveillance; subsequently a US official said that they are not collecting personal information (content), but collecting only 'meta-data' (context). The intended point was that the NSA wasn't collecting the words that we spoke during our phone conversations; instead, they collect only the phone numbers of the two parties, and the date, time and duration of the call.

Collecting metadata on people means putting them under surveillance. Imagine that you hired a private detective to eavesdrop on someone. The detective would plant bugs in that person's home, office and car. He would eavesdrop on that person's phone and computer. And you would get a report detailing that person's conversations.

Now, imagine that you asked the detective to put that person under surveillance. You would get a different, but a nevertheless comprehensive report: where he went, what he did, who he spoke with and for how long, who he wrote to, what he read, and what he purchased. That's metadata and metadata is still surveillance data.

Telephone metadata alone reveals a lot about us. The timing, length and frequency of our conversations reveal our relationships with others: our intimate friends, business associates and everyone in-between. Phone metadata reveals what and who we're interested in and what's important to us, no matter how private. It provides a window into our personalities. It yields a detailed summary of what's happening to us at any point in time.

Technology advancement comes with a price, and we have to bear it.

Over the period of time, accumulated personal data can probably paint a better picture of how you spend your time, because it doesn't have to rely on human memory. Most of us have at least one or more social network accounts, and do various activities. Adding friends, new postings, status updates, chatting, and many more activities.

Web search data is another source of intimate information that can be used for surveillance. (You can argue whether this is data or metadata. The NSA claims it's metadata because your search terms are embedded in the URLs.) We don't lie to our search engine. We're more intimate with it than with our friends, lovers or family members. We always tell it exactly what we're thinking about, in words as clear as possible. Google knows what kind of porn people search for, which old lovers we still think about, our shames, our concerns and our secrets. If Google decided to, it could figure out which of us is worried about our mental health, thinking about tax evasion, or planning to protest a particular government policy. I used to say that Google knows more about what I'm thinking of than my wife does. But that doesn't go far enough.

Google's CEO, Eric Schmidt, admitted as much in 2010: 'We know where you are. We know where you've been. We can more or less know what you're thinking about.' You may ask how do they do this? One way to think about it is that data is content, and metadata is context. When you have one person under surveillance, the contents of conversations, text messages and emails can be more important. But when you have an entire population under surveillance, the metadata is far more meaningful. Metadata can be much more revealing than data, especially when collected in aggregate.

Think about the day-to-day activities; shopping at supermarket. How many of you have privilege cards? Think of a simple activity, at the supermarket cash-till you hand over a privilege card in order to gain points that gain points so that we can redeem one day. Do you know how much personal information can be gathered by this? When we register for a privilege card, we give our name, address, contact number and much more to the supermarket. When we do our shopping, this loyalty card and credit cards are associated with our bill. By doing this we share our shopping pattern, our personal information, and our banking information. Moreover, our shopping pattern can be matched by the product companies and the special discounts.

Not only that, now we also have get wearable devices (for example, Google glass, biosensors), and internet of things devices picking up in numbers. All these devices generate data about you and surroundings. Recently Google claims their quantum computer is 100,000,000 times faster than a classical computer. In simple terms, an instruction can be executed in a hundredth of a second; with a more classical computer, it would take about 100 days.

Telephone metadata alone reveals a lot about us. The timing, length and frequency of our conversations reveal our relationships with others: our intimate friends, business associates and everyone in-between.

The human cost

Sunny Kim, an economics student from State University of New York, Albany, returned to South Korea to take up a job after graduation. However, she stayed connected with her US friends on Facebook and by using the messaging app KakaoTalk. In South Korea, she met a man who would become her boyfriend. She would regularly share snaps of them together on Facebook. Kim also regularly posted pictures of her friends, crafts, food, and her puppies to Facebook. A friend told BuzzFeed News: 'It seemed like she was happy, eating and living well.'

Kim went missing on 2 May, according to reports. On 18 May Kim's body was found in a suitcase buried in a hill. Her boyfriend confessed to her murder. Kim's sister said she didn't realise that Kim was dead at first, because Lee impersonated her for two weeks by responding to texts sent to her phone.

If Lee can impersonate his girlfriend for two weeks, it begs the question: what can a super computer do? Another question springs to mind: 'When you go out of the house and try to call home, are you really talking to your loved ones?' Such a day is not too far away...

References

NSA Surveillance and What To Do About It - Bruce Schneier **www.youtube.com/watch?v=3v9t_IoOgyI**
Bruce Schneier and Edward Snowden @ Harvard Data Privacy Symposium 1/23/15 **www.youtube.com/watch?v=7Ui3tLbzIgQ**
TalkingStickTV - Bruce Schneier - Data and Goliath **www.youtube.com/watch?v=seNHe5oMquw**
www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3
Obama about NSA **http://mashable.com/2014/06/05/edward-snowden-revelations/**
The Battle for Power on the Internet: Bruce Schneier at TEDxCambridge 2013 **www.youtube.com/watch?v=h0d_QDgl3gI**
Bruce Schneier's Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World **www.youtube.com/watch?v=eoI4WDEmF_c**
How Hackers Take Back the Web **www.hacoder.com/2015/10/how-hackers-take-back-the-web-documentary/**
Behind the Scenes: How Technology Turns Consumer Data into Actionable Insights **www.technologyreview.com/view/544326/behind-the-scenes-how-technology-turns-consumer-data-into-actionable-insights/**
Build Your Social Network Now With Facebook AI Hardware **www.hacoder.com/2015/12/build-your-social-network-now-with-facebook-ai-hardware/**



Image: iStock.com/ALotOfPeople

WINNING HEARTS AND MINDS

Jamie Randall, founder of The Friendly Nerd and Technical Director of the IASME Consortium, argues that we need to give organisations the right kind of skills to prevent data breaches.

Take a look at any newspaper from the past year and you are likely to find some terrifying facts about cyber security, generally related to massive data breaches by trusted companies or revelations about spying on citizens by friendly and not-so-friendly governments.

It's no revelation for anyone in the IT business that information within computers and servers regularly ends up in the wrong hands or goes missing. We've spent decades putting into place ways to manage systems in a predictable and authorised manner (hello ITIL) and put good risk-based controls around them to help prevent things from going wrong (good to see you ISO27001, howdy the IASME Standard). These have had a great impact and have made many companies much more secure as a result.

What we must not forget along the way is to tell the rest of the business that they should care about security too.

The government is seeking to increase skills in the cyber sector and has launched a range of initiatives to get more young people skilled up in the technical areas of cyber defense. The government is fairly good at getting the 'technical bits' of cyber security correct, and it leans on its technical security arm, the Communications-Electronics Security Group (CESG0), for much of this.

A lot of these technical elements have made their way into the basic standard for cyber security, Cyber Essentials, which is a really good starting point for many companies on their journey towards better security.

What is important in the wider approach is to provide practical knowledge and skills on cyber security to ordinary employees within companies, and this includes managers, directors and general staff. Basic errors by employees, such as sending emails to the wrong recipients, failing to encrypt USB sticks then losing them and using poor or default passwords, make up the vast majority of all data breaches reported to the ICO.

It is these sorts of cyber incidents which can cause significant harm to the individuals whose data is lost, through fraud and identity theft, and to the organisations themselves, who may lose their competitive edge if product plans or pricing information is given to competitors.

It is these low-level high-volume incidents that gradually wear away at the population's trust in online services and decrease the competitiveness of the wider UK economy.

So how do we fix it?

The good news is that actually most employees are now pretty aware of the threat of data breaches, (maybe less so the techy details of hacking), and thanks to the explosion of social media some have understand the notion of keeping safe online. The key is to tap into that basic idea of good practice at home, expand on it and bring it into the workplace.

It's important to have a clear figurehead for the messages about cyber security within your organisation. Ideally this shouldn't be the IT department because staff are weary of the lists of dos and don'ts that many IT teams will have sent out previously. HR teams work well as a source, not least because they are linked to pay (a source of motivation), policies, and often are involved in existing training. In the right company finance or even marketing can work as sources.

Put out clear messages that set expectations on security from the figurehead and keep staff updated to recent trends and incidents, perhaps via email, intranet or regular team meetings. The figurehead must be two-way. Staff should be able to ask queries about topics and also be able to report security incidents.

Regular staff training is a great way to get people on-board with your security initiative. One way could be to train directors and managers in cyber security and use them to message to wider staff via an awareness campaign. A more comprehensive method would be to provide two levels of training; practical, day-to-day advice for general staff, and strategic advice for decision makers. Use online training to support rather than replace face-to-face interactive training.

And, don't forget the Data Protection Act (DPA). Most companies have training on this already but a lot of the training seems rooted in the late-1990s, meaning it doesn't fit the wider picture of cyber security and is frankly dull. Why not refresh your DPA training to make it fit the current risks that your company faces and your wider approach to security. After all, a lot of the principles used to protect personal data under the DPA apply to all your other data within the lens of cyber security.

What should we be skilling staff to do?

Most of the skills and messages needed for general staff might look obvious for many who work in IT, but the truth is that most of us don't actually follow this good practice ourselves. The key is making advice practical and approachable. The average person has very little time in their day to mull over the cyber risk levels of each of their activities, so making advice appropriate to the organisation, and to some extent prescriptive, is key.

If all the staff in your organisation had the following five things in mind during each day, you can bet your risk of a data breach would be significantly lower:

- Remember that data has a value in both financial terms, to criminals and hackers, and in terms of the harm that could be caused if it was lost or damaged. Treat customers and company data with the same care you would expect a company to treat your own private information. Think of the impact on you if your cloud provider lost all of your family photos or accidentally posted your private documents on social media
- Understand that people want to steal or damage company data. Be wary of responding to urgent emails with attachments or entering your login details into an unexpected pop-up window. Think about if this might be an attempt to steal data and ask your manager or colleagues for a second opinion
- Think in terms of how important a particular piece of information is and whether it needs extra protection. A simple data classification scheme can provide great guidance together with a table of actions to refer to – if it's sensitive data then perhaps it must be encrypted before emailing or being sent by post
- Be prepared to question things. If there is someone wandering around the office that you don't recognise, ask who they are
- Think twice before sending out information and verify the recipient is correct. You can set your email client to delay sending messages for a few minutes after you press send to give you a second chance, if needed
- When you are out of the office, use a virtual private network (VPN) to keep safe on Wi-Fi hotspots and be more aware of your privacy and security. Keep laptops and tablets with you all the time in your hand luggage – don't leave them in the car boot.

The government is seeking to increase skills in the cyber sector and has launched a range of initiatives to get more young people skilled up in the technical areas of cyber defense.

Turning these sort of basic principles into practical advice that is suitable for your organisation requires some work, but not really that much. Perhaps a few afternoons in meetings and the odd heated discussion on the details and most companies will have some great practical advice to share with their staff that fits their work environment.

And that's a lot better than weeks of late nights spent trying to resolve the headache of a data breach.



BEYOND ANTIVIRUS: LAYERED SECURITY

Stuart Clarke, Information Technology Security Officer, Hampshire Constabulary and Thames Valley Police, confirms that dealing with the insider threat is a tricky business, one that involves a number of technical measures.

Image: iStock.com/neverarp

For the purpose of this paper, a malicious insider is defined as a current or former employee, contractor or business partner who meets the following criteria:

- Has or had authorised access to the organisation's network, system or data
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity or availability of the organisation's information or information systems.*

According to surveys, the most common insider threats are:-

- Unauthorised access to or use of an organisation's information
- Unintentional exposure of private or sensitive data
- Viruses, worms or other malicious code.

In order to protect an organisation a layered security approach is best adopted such that any deliberate or accidental injection of any none official software or hardware or unauthorised access to information can be readily stopped or detected and quickly handled. There are many others involved in the handling of the outsider threat, but the main areas used for the insider aspect are described below.

Enforcement of separation

The technical estate should be divided into individual logical areas that only those that are required to have access can gain access to so, for example, a member of HR has no need to see the information relating to finance and should, therefore, not automatically be given such. All such access should be controlled via a logged service request procedure and should require someone with administrator access to change.

Enforcement of least privilege

This well-known data handling methodology is also adapted into the technical aspect by using security groups and controls to ensure staff are only able to gain access to data in the correct areas required for their work, irrespective of their location or seniority. Exceptions could be permitted but, again, this should require a service request and a member of staff with administrator level privileges.

If necessary this should follow the principles of the Government Security Classification Scheme (GSCS), which employs the principle of 'need to know', the requirement for defence in depth and the segregation of sensitive material that can also be technically employed.

Strict password and account management

Leading on from above, the creation and modification of accounts should be strictly controlled by a small set of users with escalated privileges such that on ingress into the organisation their account should be created by this group and will be based on a known set of base accesses relevant to the role they take. Modification of that can take place but again this would require that escalated privilege which should not be granted by default but by relevance to role.

Logging and monitoring of unusual actions

Throughout the networks there should be numerous monitoring systems in place that record and audit user activity. These cover aspects from what communications pass into and out of the network to where and whom logged in to specific devices at specific times. Different and varied restricted groups of staff should be able to alter what can be stored therein and have access to that information and are alerted to or alert about anomalies.

Active defence against malicious code

The organisation should employ highly sophisticated and well-structured defences against malicious software. The opening of any file should trigger the scanning by an anti-malware package, which may vary according to platform. You should also run anti-malware scans across the whole of the organisation in a constantly rotating cycle such that even a file that has not been opened for some time will be scanned. Any alert should then lead to a trigger to a number of specific and trained staff within ICT and information security and to the monitored management consoles.

However, all anti-malware packages are reliant upon the signature files that are provided by the systems provider. Systems should receive such from suppliers more or less as soon as they are released and begin to distribute these quickly. Indeed the log on process should include ensuring the latest is installed and, for remote devices, extend to refusing log on if it has not been achieved for a predetermined period of time. The update of the new signature files should be recorded by the management systems of these and monitored by the relevant staff.

However, not all malware is known at the time of exposure and the anti-malware software should also employ host intrusion prevention systems (HIPS) that monitor the running of software and look for behaviours consistent with the actions of malware and, if necessary, raise an alert. This is learning software that gets to understand and baseline the activities of a system over time, becoming ever more accurate.

Patching policies

Following on from the above, most malware exploits an existing and known software vulnerability. Therefore it is essential to ensure that the software is patched up-to-date to ensure that it cannot be exploited. For example, the Conficker virus, although possibly devastating, is very easily resolved by ensuring the correct patch is in place.

To that end organisations should employ a strict patching policy to ensure that software is updated as quickly and efficiently as possible, and these be monitored by management software that reports back on the success rate of these being installed. Again ensuring equipment is patched up to date should be part of the log on process.

Internet access controls and monitoring

A good percentage of malicious software requires the ability to be able to communicate out and back in to the organisation it is attacking. The organisation's access to the internet should be controlled by the use of hardware that analyses all communication and will strictly block access to or from unacceptable sites.

Again, as well as the manual choices to not allow access to certain types of sites, a list is maintained and updated to the equipment to ensure that it contains the latest information regarding sites that may be being used for the wrong sort of communications.

Access and control to this hardware and its black and white lists should, again, be strictly controlled and granted on role requirement rather than individual.

Strict termination policies

When a person is no longer deemed to be working for the organisation the HR department should mark this in their systems and this trigger a number of automatic e-mails that are sent out to various teams in order for certain events to take place. It should also mark their systems appropriately as these may also be accessed by other staff to ensure access validity. Also this should include physical access control systems to stop any physical access method working.

In the IT department this should lead to an immediate suspension of the log on account so that it is not possible to log on to their account. Also asset management teams can start the process of device recovery, if necessary, and can suspend accounts on devices such as mobile phones, if required.

Secure backup and recovery processes

As is expected with any organisation handling sensitive information there should be strict backup policies for all critical systems using a number of techniques and media, mainly running on a rotational basis to separate media that should then be stored in secure off site locations. Indeed certain members of IT staff should have strict responsibilities to ensure these are completed on a daily basis.

Then, should an issue occur, well-kept records should enable recovery of data from specific points in time via tried and tested recovery procedures. These should also be periodically checked to ensure the backups are working properly and that the procedures will work if required.

Baseline of normal network behaviour

With most of these systems there should be a known and accepted baseline from which unusual actions can be spotted and action taken. Subject matter experts in IT, who work with the systems on a daily basis, have an understanding of the normal behaviour of the systems they work with and should be able to document this and quickly spot and investigate issues when they deviate from the norm.

Dealing with the insider threat is a complex business that involves a number of technical measures, but also relies on a number of departments within an organisation working together to ensure that the risk is mitigated.

Further reading

* 'Common Sense Guide to Mitigating Insider Threats - 4th Edition' – Software Engineering Institute – December 2012)



Image: iStock.com/milan

THREAT INTELLIGENCE CHALLENGES

David Strudwick MBCS, CyberDefence Dynamics, highlights several threat intelligence challenges and explains why businesses need to make the most of such threat intelligence.

In the context of the cyber domain, threat intelligence (TI) endeavours to describe how computers might be at risk of attack or misuse in facilitating various types of hostility (in a conceptual battle-space). Expressed in simplest terms, TI is the product of timely, relevant information and its meaningful evaluation in terms of the probability of attack, the vulnerability of systems, the capability of attackers, their motivation, opportunity for exploitation and the likely severity of impact.

Couple all these with an extra factor that TI tends to be functionally non-compositional, and it looks a complex affair, but easy when one knows how.

Application

Properly applied TI guides configuration of security controls in concordance with an overall defence posture. (Although beyond the scope of this report, TI also assists in alignment of technical capability in business continuity, disaster recovery, data management, interoperability and many aspects of legal and regulatory compliance). Applied TI should collectively achieve the two critical goals of battle-space situational awareness and commensurate response to diminish an attacker's available time and resource envelopes. Within the cyber domain, a TI development cycle with underpinning toolsets would seem critical.

Intelligence collection

Authority is crucial in TI collection; that curious amalgam of capability, knowledge of and influence over a given computing arena, and is essential for selecting intelligence sources. TI must be relevant, its veracity and trustworthiness tested and triangulated against a bridgehead of demonstrable facts; any interpretation should avoid inaccuracy, dangerously insidious bias4 or deliberate deception.

Proximity of sources is everything. The value of TI arising from within an organisation's own technical domain arises by virtue of its dependability. Products such as LogRhythm are particularly adept at gleaning actionable TI by interrogation of the organisation's aggregated logs, parsing, analysing and reacting to seemingly innocent event data that when conjoined, alert possible indicators or compromise.

But serious insider threat might be more subtle; a laissez faire attitude to security amongst those with influence (or even keen maintaining the status quo) is a more dangerous internal threat, and technically undetectable.

Disparate non-human sources of TI

Specialist tools such as Darktrace are self-tuning/configuring, employing advanced statistical analysis of internal network traffic. Acting like a biological immune system, over time it detects subtle deviations from normal network interoperability and user activity. External network interaction in real time can be assessed by tools such as FireEye 6 identifying anomalous traffic, data types and sources across a variety of domains and applications. In concert, (with well-practised process) these tools may rapidly direct attention to the tell-tale signs of miss-configuration or, more importantly, exploitative, capable threat actor's presence.

Open sources

Much benefit can be gleaned from reliable dialogue with networks of computing emergency response teams (CERTs) and warning, advice and reporting points(WARPs) or even international feeds from US National Vulnerability Database run by National Institute of Science and Technology(NIST).

Gathering open source intelligence is often fruitful, especially the recognition and location of lost data (possibly even for sale!) or novel exploits applicable to known and pertinent vulnerabilities that could be deployed by capable and motivated threat actors. Access to a private global threat intelligence network (e.g. the service offering from FireEye) presents the possibility of immediate notification of newly discovered indicators of compromise.

When such response is integrated into the prevailing configuration of their worldwide client-base, this functionality reduces the probability and severity of pending attack down the line, or perhaps enabling discovery of a latent threat vector buried away within extant data or processes.

Similarly, historic threats often re-surface, but newly repackaged, recombined and re-blended after years of quiescence. More worryingly, attack on critical SCADA systems necessarily implies that critical national infrastructure (CNI) is unlikely to be exempt from sophisticated cyber attackers and consequently, must attract both considerable threat intelligence effort and highly robust response at government level.

The extreme complexity, severity and adverse impact implies that such attacks will be zero-day in nature and directed against the very highest value assets and processes.

Volumes of data

Automated processes underlying threat intelligence analysis usually requires the collection and processing of very large amounts of data, the vast majority being totally benign in nature. The challenge is finding the needle (or even just that blade of straw!) in the haystack; this is often seen as the greatest detraction to undertaking threat intelligence programmes.

The collection of disparate data sources presents considerable challenges for some organisations, testing their technical capabilities to the limit. Many organisations give up and consequently, their aforementioned authority exists in name only.

Unfortunately, gathering critical TI sources is like potty training; any parent will testify that persistence is critical and success is vital (and non-negotiable!) if serious organisations are to be truly responsive, functioning and properly contributing to the internet society.

Once underpinning data is collectable, timing is everything; data aggregation presents other issues because subtle extraneous factors (such as event simultaneity) are critical in intelligence assessment. Furthermore, there are legal hurdles to overcome; response must be proportionate and lawful.

Response and actionable intelligence

In formulating and invoking commensurate cyber response, if there is no meaningful TI capability, then the organisation is at best partially sighted, or at worst, driving blind. An effective TI programme manoeuvres an organisation from knee-jerk, reactive, fire-fighting to greater proactivity, observing and nipping potential problems in the bud.

Without behavioural data from systems, an organisation's TI function will be impossible to realise. There will be little opportunity to expose indicators of compromise generated by threat actors. Response will be impaired, if not impossible and formal compliance with security incident management sub-systems and other regulatory compliance will be muted.

In conclusion, to provide most benefit, the TI cycle must be linked with analytical/forensic processes that blend intelligence sources. Vital evidence from aggregated network device logs, security enforcing systems, applications software, database architecture and other business services, if handled properly and responsibly, may even be admissible in court.

While such endeavours are rarely non-trivial they will test even hardened professionals. However, effective intelligence-led security management is said to enhance both trustworthiness and corporate reputation, thus providing clear wealth generation benefits from such positive market differentiation.

Further reading

1. In the context of this article, risk is the probability of a threat actor successfully employing their capability, resources and vector(s), to engineer opportunity for exploitation of vulnerability resulting in adverse/severe impact, and that probability can either be tolerated, transferred, treated, transmuted or the venture completely terminated.
2. Defence posture is usually expressed in terms of notifiable events, logical rules, risk thresholds and anomalous activity with reference to the 5-Ts of risk management (as in footnote 1 above).
3. SANS Institute InfoSec Reading Room - Tools and Standards for Cyber Threat Intelligence Projects (Author: Greg Farnham Advisor: Kees Leune).
4. **www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf**
5. **https://logrhythm.com** – SIEM Security Analytics and Log Management
6. **www.darktrace.com** Employing advanced recursive Bayesian estimation to statistical network behavioural analytics.
7. **www.fireeye.com/index.html** – Adaptive approach to cyber threats.
8. **www.cert.gov.uk/resources/advisories/**
9. **www.warpnetwork.org/index.html**
10. **https://nvd.nist.gov**
11. Supervisory Control And Data Acquisition attacks - **www.computerworld.com/article/2473941/cybercrime-hacking/brute-force-cyberattacks-against-critical-infrastructure--energy-industry-intens.html**
12. IT Now - Critical Infrastructure Under Attack – Dec.'14 – Richard Piggin
13. GPG24 - The HM Government Security Incident Management Process
14. GPG18 - The HM Government Forensic Readiness standard



Image: iStock.com/Wavebreakmedia

THE AGE OF THE SoC

David Bird MBCS CITP explains why using security operations centre (SoC) services can be a beneficial investment for many organisations.

The recent series of security breaches at TalkTalk, amongst others this year, have demonstrated the newsworthy impact from the loss of reputation in the public domain. Press reporting and speculation surmises that hackers attacked and exfiltrated personal data via TalkTalk's web services using an SQL attack method. According to the company customer data loss was not as bad as it first appeared with 156,959 details compromised, rather than the four million that had been initially feared.

Although TalkTalk reacted to this event, the horse had already bolted; inevitably the damage had been done costing the company £35m as well as yet unquantifiable future lost earnings. This scenario highlights the importance of security event detection and effective incident response measures.

Organisations should not just have well architected and zoned infrastructures, security appliances, in-built intrusion prevention/detection devices forming their defence, they should have effective protective monitoring and security incident management too. The above scenario reinforces the importance of defence-in-depth incorporating organisational strategies for the detection of unauthorised intrusions and the associated incident response paradigm. This is particularly important since effective cyberattacks are now becoming common place from hackers, organised crime as well as nation states.

An answer to this ever increasing problem is the use of security operations centre (SoC) based computer network device (CND) approaches. Whether organic within an organisation or contracted through an outsourced specialist, using SoC services can be an investment for the more savvy of organisations.

The rise – a concise UK history

The dawn of the SoC age can be traced back to the end of the 20th Century in the US. In 1988 the fledgling Computer Emergency Response Team (CERT) Coordination Center was spawned at Carnegie Mellon University as a direct result of the Morris Worm outbreak. This model was swiftly followed in 1992 by the establishment of a Cyber Security Incident Response Team (CSIRT) in Europe.

With momentum being built up, by early-to-mid 2000 the UK Ministry of Defence decided to stand-up the Global Operations Security Control Centre - part of the CND and Information Communications Services strategy for Defence. By 2007 Her Majesty's Government (HMG) had set up GovCERTUK as an IT incident reporting chain for the public sector, followed by the Cyber Security Operations Centre in line with then 2009 UK Cyber Security Strategy.

Similarly security-focused commercial companies realised the potential for providing skilled SoC services as defined by the Mitre Corporation to both government departments and companies alike. By 2012 the Cyber Incident Response service was set up, in response to the 2011 UK National Cyber Security Strategy, to provide incident response services for industry supplying critical national infrastructure (CNI).

More recently the creation of CERT-UK was justifiable, undoubtedly spurred on by recognition of the impacts that can be inflicted by weaponised malware; as well as other prolific attacks that have ensued upon both the public and private sectors. Operational in 2014, CERT-UK is the single point of contact for CNI service companies, HMG and the rest of industry energised by the Cyber Security Information Sharing Partnership (CiSP).

This latter framework has been set up to fuse threat and vulnerability information from industry and government alike - an approach that complies with the 2013 European Union Network and Information Security Directive. All of these capabilities provide the UK with the key ingredients for a heterogeneously meshed CND infrastructure.

Making sense of it all

That said, experience suggests that all too often protective monitoring has been seen by some technocrats as a business as usual overhead or embuggerance to the uninitiated. Thus actionable CND and threat intelligence may appear intangible to some until the worst happens. At the end of the day the consequences of the lack of protective monitoring could enable:

- Sensitive information to be abused or intellectual property to be leaked by malicious insiders; or
- Unauthorised trade secret acquisition may be conducted illegally through advanced and persistent threat incursions and/or prolonged cyber espionage activities.

In mitigation SoC systems and analysts can provide benefits such as:

- Ensuring that system logs and network flow statistics are reliably processed in a timely manner
- Vulnerabilities can be assessed with specifically crafted toolkits or deployed agents to drive patching/configuration remediation activities
- Network traffic ingress and egress and application functions can be trended in order to detect abnormal or suspicious activities
- Machine-learning and events analytics enabling sensor fired false positives to be tuned-out.

From a vendor agnostic viewpoint, technology is not the panacea that is expected even with these capabilities designed or bought-in, and security information event management technologies deployed. A key ingredient is the all-important derived threat intelligence aspect underpinned by contextualised audit and accounting reporting of associated data feeds.

Outputs need to be interpreted so that tailored reports can be issued and mature escalation paths devised; where actionable information should not just be contained within the operational security team, but also communicated to service management teams ; thereby ensuring that holistic and informed reactive decisions can be made. Enterprises also need to weigh up SoC benefits to include:

- The best fit technology and service wrap against the cost
- Legal admissibility of proportionately accumulated and collated evidential data
- When outsourcing, assess the maturity of any SoC specialists to include protection of customer data especially when the outsourcer may be providing services to multiple clients.

For example, the US National Oceanic and Atmospheric Administration (NOAA) is a case study of an enterprise that has successfully embraced incident response. In the past this national weather service had been plagued by bad security practices across its networked systems that control a constellation of weather and photographic satellites. However, their chief information officer had the foresight to implement a SoC infrastructure. During the much publicised cyberattack of late 2014 this SoC's CSIRT was undoubtedly involved in the intrusion detection and was influential in conducting an unscheduled outage - to implement what could be construed from press reporting as vulnerability remediation.

The future

Organisations will not know whether they are under attack from outside or from within without efficient, proactive vulnerability and threat intelligence, supported by defined incident response procedures. A combination of technology and data feeds - ranging from the edge boundaries to inside the enterprise perimeter - and processes have a better chance of detecting nefarious activities.

Recently the Information Security Media Group (ISMG) and FireEye conducted a breach preparedness and response study from a survey population of 260 mid-to-large organisations. A striking statistic was that 67 per cent of the respondents rated their incident response skills as average or below – this is seven per cent up from a similar category of incident response effectiveness in the joint ISMG/FireEye Need for Speed Survey of 2013. So awareness for such capabilities is gaining traction.

With the adoption of cloud computing, and the advent of software defined networking, the monitoring paradigm across multiple OSI layers needs to be taken very seriously. This is on the basis that infrastructure not only comprises the networks, it has now enveloped the nodal hosts and hypervisors of this virtualised dimension. This would enable near real-time monitoring of logs/events from these elements to ensure software-based exploitable vulnerabilities can be plugged when patchable - hindering hitherto unknown or opportunistic attacks from evading detection and thereby impede onward propagation. To thwart today's adversaries, tomorrows SoCs must not just concentrate on the network layer, but also incorporate responsible monitoring of both the host servers and virtualised cloud server/desktop instantiations.

References

1. Tara Shields, 2015, #TalkTalk: SQL Injection Possible Attack Vector for ISP Breach, 2015, **www.information-security-magazine/news/she-injection-possible-attack-vector-for/**
2. TalkTalk, Cyber Attack update – Friday November 06th 2015, **www.talktalkgroup.com/press/press-releases/2015/cyber-attack-update-november-06-2015.aspx**
3. BBC, 2015, TalkTalk cyber-attack: Website hit by 'significant' breach, **www.bbc.co.uk/news/uk-34611857**
4. BBC, 2015, TalkTalk hack to cost up to £35m, **www.bbc.co.uk/news/uk-34784980**
5. CERT Software Engineering Institute, 2015, Carnegie Mellon University, **www.cert.org/about/**
6. ENISA, 2015, **www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt**
7. Defence Committee, 2013, Further Written Evidence from the MoD, **www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106we05.htm**
8. Carson Zimmerman, 2014, Ten Strategies of a World-class Cybersecurity Operations Center, Mitre
9. CPNI, 2015, Cyber Incident Response Services, **www.cpni.gov.uk/advice/cyber/cir/**
10. CESG, 2012, New Cyber Incident Response scheme launched, **www.cesg.gov.uk/News/Pages/Cyber-Incidence-Response.aspx**
11. Stephen Cobb, 2012, 'Broken trust: Nation-state malware has a negative impact on GDP' **http://betanews.com/2012/06/14/broken-trust-nation-state-malware-has-a-negative-impact-on-gdp/**
12. CiSP, 2014, CiSP, **https://www.cert.gov.uk/cisp/**
13. Charlotte Walker-Osborn, 2014, EU Cybersecurity Directive, BCS ITNow Magazine.
14. Adam Wood, 2014, Fail to Prepare, Prepare to Fail, BCS ITNOW Magazine.
15. NOAA CIO, 2011, FY 2012 – 2016 National Oceanic and Atmospheric Administration Strategic Information Technology Plan version 3.
16. Mike Gruss, 2015, NOAA Admits to Cyberattack on Satellite Data Networks, **http://spacenews.com/42561noaa-admits-to-cyberattack-on-satellite-data-networks/**



Image: iStock.com/michele piacquadio

SHARED SECRETS

Andrew Hay, Director of Search Research, OpenDNS, provides an overview of the shared secrets of malware authors via the 'dark art' of Steganography.

Steganography has a long and colourful history. While you might not have known its name, the technique has been used for centuries by militaries and intelligence operations around the world in a variety of low tech ways.

Commonly a plot device in mystery shows, a message is written in invisible ink on the back of a real letter. When the intended recipient gets the letter, they gently heat it up, revealing the message. Anyone else who has the letter is generally unaware there's a hidden message on the back.

That's steganography – the practice of hiding a message inside of another message. While this basic premise is fairly common, we've recently seen a resurgence in steganography's usage among a new audience – malware authors.

The system

Before we dive into how malware authors are leveraging this technique, let's take a deeper look at the advantages and disadvantages of steganography.

The system relies on a shared secret with two pieces of information: that the message exists and how to reveal the message. Hence, if I want to communicate with you, the reader, in secret, after our initial meeting we decide on a method of hiding messages to each other.

We're going to use the first letter of each word in a paragraph:

Howard called Edward after school.
Edward, expecting the call, answered on the second ring.
Laughing at a shared joke, they quickly started to discuss their science fair project.
Last year, Julie won the fair with a twist on the classic baking soda volcano.
Once they discussed why her presentation was so effective, they started to figure out how to win the top prize.

Besides being an utterly horrid piece of writing (yes, it's original), this paragraph serves our purpose well. Hidden in the completely mundane writing is our message. By taking the first letter of each word, we recreate the message, 'H E L L O'.

Since we knew how the message was concealed, it was easy to reveal.
This also highlights steganography's biggest weakness. If you know of the existence of the message you can easily intercept it. The strength of the system is in how much noise is around the actual message and how well the message is hidden within that noise.

What about encryption?

This differs from encryption. In a scenario involving encryption, outsiders (not the sender or recipient(s)) are aware that the message exists, they simply can't decipher it.

The same example: **M J Q Q T**

We've 'encrypted' this using a simple shift cipher (which is so easy to break you should never use it outside of this type of example). The ASCII value1 of each letter was incremented by five (H = 72 + 5 = 77 = M) to produce our cipher text. Since it's such a short message, it's ridiculously easy to crack by hand, but the point is the same. Encryption doesn't hide the fact that there's a message, it just tries to make that message very hard to read.

In the digital world

We've seen steganography's use in the physical world. Let's a take a look at its use in the digital world, where it really starts to shine.

It turns out that a lots of very common file formats can safely have additional information stored inside the file without affecting that file's normal functions.

Take for example, the first photo on the following page (Image 1), It's a simple JPEG of a mountain scene. However, when you run it through a decoding tool, you'll find a hidden message. There is a subtle difference in the file from the original and the one containing the message, but it's not a difference that you would see or one that a tool would find unless it was specifically built to look for it. The below image (Image 2) shows where in the file the hidden message is encoded.

Even knowing where to look you won't find any visual differences. The message is hidden in the areas of the digital file that don't impact its primary content.

Evading detection

Because steganography uses slack space and other areas of these common file formats, but doesn't affect the content itself, it is extremely difficult to detect.

Most security tools we use in the active defence of our organisations do not look for data hidden using steganography. That's not to say that it's impossible to detect messages hidden using these techniques. There are a number of tools that can help in a forensics investigation, but they are very time consuming to use and don't guarantee detection.

Given these constraints, it simply isn't practical to scan every file entering or leaving an organisation for hidden material. This makes steganography a very powerful technique to get data past existing defences.

New uses

Fortunately, steganography was really only seen during in-depth investigations. It is rare, but not unheard of, to come across examples of steganography during in-depth investigations of specifically targeted attacks, collusion, or other multi-party investigations.

That has started to change. Recently, we've seen more and more malware authors are taking advantage of steganography in a number of ways. It was first noticed with a piece of malware named Duqu. This complex malware sometimes hides encrypted information inside JPEG images, it then sends out of an infected network, easily bypassing any content filtering.

In 2014, French researcher Xylitol, discovered that a variant of the Zeus malware (ZeusVM) was using steganography to hide commands it was sending to infected machines.

Last summer, Brett Stone-Gross at Dell Secureworks discovered that the Lurk Campaign took the ZeusVM technique to its logical conclusion. This downloader now delivers other malware via steganographic techniques.

More recently, the team at Dell Secureworks analysed Stegoloader which shows just how rapidly malware authors are incorporating these techniques into their products. This malware uses a suite of counter-forensic techniques to avoid detection and eventually downloads additional functionality hidden in a PNG file.

As more malware authors see tangible benefits from leveraging steganographic techniques, they will quickly become widespread.

Challenges

Data hidden using only steganography can be extremely difficult to detect. The performance challenges of scanning almost every file for small, non-impacting anomalies are huge. It's just not practical to check every file coming in and out of an organisation at the depth required.

That has created an opportunity that we have seen malware authors taking advantage of. To date, we've seen steganography used to:

- Hide data leaving an organisation
- Covertly send commands to infected machines
- Smuggle malware across existing defences.

More examples are being found as these criminals see the very real advantages of this technique. Defenders and the security industry are racing to catch up. The best current defence is to attempt to prevent infection in the first place.

A strong security practice focusing on actively monitoring, strong access controls to your data, and one that continues to invest in its people is the best approach for now.

There should be a more positive note to end this on. Sadly, there isn't, but if you can think of one, let me know via Twitter where I'm **@andrewsmhay**

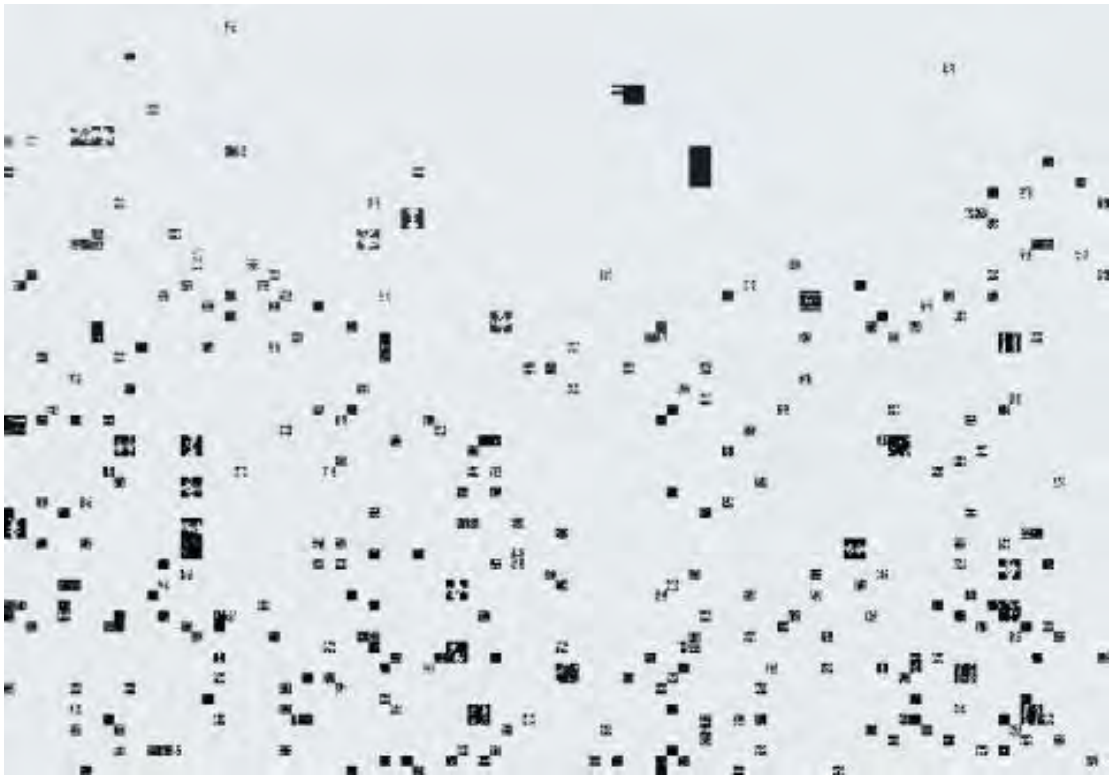
References

1 **www.asciitable.com/**
2 **https://en.wikipedia.org/wiki/Duqu**
3 **www.technologyreview.com/s/529071/the-growing-threat-of-network-based-steganography/**
4 **https://en.wikipedia.org/wiki/Zeus_(malware)**
5 **www.theregister.co.uk/2014/02/20/zeus_bank_hackers_hiding_malware_controls_in_jpg_in_a_nod_to_the_ancients/**
6 **www.secureworks.com/research/malware-analysis-of-the-lurk-downloader?view=Standard**
7 **www.darkreading.com/endpoint/attack-harbors-malware-in-images/d/d-id/1297867**
8 **www.secureworks.com/research/stegoloader-a-stealthy-information-stealer**
9 **www.securityweek.com/information-stealing-malware-%E2%80%9Cstegoloader%E2%80%9D-hides-image-file**
10 **http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/**

Image 1.



Image 2.



Images supplied by Andrew Hey



Image: iStock.com/ismagilov

INCIDENT MANAGEMENT

Steve Daniels FBCS CITP, Strategic Business Advisor for Cyber Security at CGI, in the UK, considers the importance of structured and considered incident response and lesson learning to improving security.

As the number, frequency and scale of cyber-attacks and breaches increase, the need for a professional focus upon incident management also grows. For quite some time now, this area has been characterised by a relative lack of focus, low standards and a temptation to deploy 'Superman' behaviours – such as over-loading of professionals for long hours, rather than to plan and rehearse carefully. This has underpinned a poor perception of the security of IT services and held back their wider public adoption.

But the position is not as bleak as it is routinely painted. With new standards (such as BS65000 Resilience, BS11200 Crisis Management, ISO27035 Incident Management and ISO27013 – Integration of IT and Information Security Management), there is a growing set of guidance and requirements materials with which to respond to the calls for improvement from partners, the public and regulators.

More significant than the indirect benefits of addressing this issue, incident management can deliver such a level of direct benefits that, if there was one maturity improvement that enterprises should prioritise in 2016, it would be this.

A vital component of every information security management system (ISMS)

Whether the objective is compliance or formal certification, the adoption of ISO27001 (and 002) clearly continues apace, with the implementation of information security management systems (that embody Deming's 'Plan – Do – Check – Act' model) to demonstrate effective cyber security. An ISMS / PDCA model will only ever function poorly without effective incident management, by leaving lessons unlearnt, impacts unreduced, risk assessments un-un-acted on and control frameworks incomplete or even – though much more rarely – excessive.

Indeed, within a year or two there will be the new EU Data Protection and Network Information Systems Directives to comply with, with their embedded requirements for mandatory reporting. It is already clear that active compliance will be needed, and that breach is likely to incur a material level of fines. Weak incident management will drive new, additional and avoidable costs.

Working with the organisation

The most common mistake in incident management is organisations treating the activity as a technical or IT matter relating to system availability, when it is actually an organisational issue with service delivery or business consequences. The response required therefore almost always has a wider focus.

Who will do what when the organisation is hacked and emails threatening to expose corporate secrets are received? Who needs to be contacted to provide what support? How will operations be sustained? Who talks to the media, customers, champions, lobby groups and regulators? These are all questions for consideration.

Incident? What incident?

As with every other part of the ISMS, cyber security is essentially a risk management discipline, incident management needs to be calibrated by the risks, whether that is the assessment and prioritisation of events (i.e. what the likely failure scenarios are expected to be, exactly what constitutes a 'P1' etc. in this case?) or the form, mechanisms and immediacy of response.

Another common failure seen is to either segment or process security incidents from other incidents differently. But this should be limited wherever possible or at least whilst the organisation increases its capability. After all, many incidents will imply a loss of confidentiality, integrity or availability and will be of interest to the CISO.

On the other hand it isn't feasible for all incidents to be reviewed by all parties, in parallel and at once, especially where there are demanding availability levels and data loss goals to deliver. In such situations, a well-defined process will be needed to allow immediate response to major incidents, including perhaps invocation of DR by IT operations, with the subsequent, higher level, incident management. This is sometimes best delivered by the security function, or with them playing a central part, to exploit their operational 'neutrality' as well as their understanding of the underlying risks, past risk acceptance and status of controls (that were presumably insufficient).

Aligning incident management

Using risk techniques within process planning and definition also makes it possible to align and optimise incident response and management with parallel and related activities, such as:

- Shaping and scaling, in terms of frequency and rigour, incident management, business continuity, disaster recovery and crisis management testing and rehearsals
- The integration of security operations centre (SOC) and advanced threat monitoring, for pro-active analysis, reporting and warning
- Investigations including forensics
- Seamless execution of service and business continuity management - and even crisis management – processes
- Documentation that is as specific as necessary, yet as generic and out-comes-focussed as possible, to allow skilled personnel to respond flexibly
- Planning, scoping, aligning and integration of reactive and pro-active
- Lesson learning
- Maintaining the currency and accuracy of ISMS documentation e.g. the statement of applicability and integrated compliance reporting, achieved using such platforms as AcuityRM's STREAM product.

The right people, at the right time

An incident, with its resulting uncertainties, all too often encourages 'random' reaction (as against a flexible response by experienced personnel) and a certain 'fog of war'. This is to be avoided or minimised at all costs.

The understanding of risks and their associated scenarios, mapped into incident priority, and response levels, provides a powerful mechanism to drive the right engagements. After all, if an incident is classified as the proverbial 'P1', it is also a crisis in waiting, if not properly managed.

Considering the risks carefully, it is entirely possible to ensure that:

- There is full clarity of roles responsibilities
- Management of the incident is immediately escalated to the operational levels needed to drive a successful response, both in the provider's and the service customer's organisations
- Organisational governance and technical oversight is implemented
- Response 'time windows' / default escalation points are complied with.

Recover yes – but follow through!

As the 'fog' recedes there is an understandable temptation to think that the job is over, but getting the best out of incident management requires a solid follow through. There are evolving reporting obligations to be met, but effective reporting can be used to enhance perceptions of security, not just restore what went before.

The collated incident management reporting (and individual incident reports) is the best means through which to finally support the ISMS's act by:

- Providing updated compliance feed-back and evidence of service level attainment
- Supporting 'tactical' lesson learning e.g. about internal process and behavioural improvements
- Identifying and agreeing what new threat intelligence has been created that can be shared through approved channels, such as CPNI's Information Exchanges or CERT-UK's Cyber-security Information Sharing Partnership (CiSP)
- Refreshing the appropriate risk models and therefore bolstering the consensus about those risks across the stakeholders involved
- Refining the incident management prioritisation and associated scenarios
- Initiating any updating of disaster recovery updates, service and business continuity strategy and plans and crisis management arrangements justified by the incidents' analysis.

Reducing the impact

Justify security resources and controls as well as, in an outsourcing environment, support the case for and against service credits and justifying spends and managing charges. All of this shows that the management of incidents is indeed a critically important and beneficial cyber security control, that is under-delivered today, ignored at our peril and entirely actionable. It is also one of the few means at the disposal of CISOs to keep some degree of pace with the threats and aim to reduce the number and duration of attacks and impact on operations.

To find out more about CGI in cyber security visit www.cgi-group.co.uk/cyber



Image: iStock.com/teolintang

ATTACKED FROM THE INSIDE

David Double MBCS raises some interesting questions as to who and what actually constitutes an insider threat.

Let me begin by asking you a question: Who today is responsible for information security within your organisation? The answer to the question of course is 'everyone', and I expect that every one of you nailed it right away. Most likely you gave it no thought at all; it is a question familiar to anyone who has worked in medium to large enterprises in recent times, and not just to staff directly involved in information risk and security. It is a question often posed during information security staff training. The type of training that is conducted for regulatory and compliance purposes, but regardless constitutes a sensible activity to include in any firm's information security arsenal,

Less often, though, is much consideration given to the implications of the answer. To illustrate, let us ask a different question:
Who today is representing an information security threat within your organisation?
It is my belief that the answer to both questions is one and the same.

An insider threat is malicious by definition, and that is certainly the traditional way such threats are viewed. A judicious starting point when considering the necessary counter-measures you will require in dealing with insider threats. It is a truism that no organisation in the world can survive without at least one trusted employee, but any trusted employee can at a later stage become a malicious one.

For a while, naïve friends I knew working in the City around this time, made a special point of looking under their keyboards each day when they arrived at work.

Easy access

In the sensational 2015 Hatton Garden safe deposit burglary, the criminal gang responsible almost got away with stealing up to £200m worth of valuables. Most of the culprits have been caught, convicted and are currently serving time in one of Her Majesty's prisons. Despite popular assumptions at the time, there is no evidence that any of these individuals, were in anyway connected with the firm from which they stole. Curiously enough I had a men's watch stored there, which unsurprisingly was not stolen, but from which I was prevented from retrieving whilst the site remained a crime scene. Proof that the impact of such maleficence can be far reaching, but I digress.

In 2009 a gang of criminals were likewise imprisoned for attempting to steal an even vaster amount of money. It was widely reported that cleaning staff at the Sumitomo Mitsui Bank in London had installed 'keystroke loggers' on various computers during their evening shift, a period when most of the office staff had left for the day.

For a while, naïve friends I knew working in the City around this time, made a special point of looking under their keyboards each day when they arrived at work. They were checking for any conspicuous device attached to their PC's, silently recording their every action. But the truth was the keystroke loggers were in fact just small programs installed via a USB stick, and the much maligned cleaners were proven to be entirely innocent.

The real perpetrators were actually met at reception, made welcome and signed in by a senior employee of the bank's security staff. They were then entirely at liberty to install the keystroke logging software at appropriate workstations. One can imagine the malicious insider pointing out the desks of the most pertinent employees in which to focus their attacks. Those possessing sufficient system access privileges, that once compromised, permitted the mooted and rather complex financial exploit to take place.

The real perpetrators were actually met at reception, made welcome and signed in by a senior employee of the bank's security staff.

It is notable that neither the inside actor nor the outside hackers supplied the data so essential for the compromising of the accounts, and crucial for the commissioning of the crime. That information was provided, albeit unwittingly, entirely by benign members of staff obligingly entering their usernames and passwords for the malicious software to capture.

So you see, in this sense, any employee can represent an insider threat, and this absolutely includes the most benevolent and good-willed members of your organisation. This is why ongoing education and training, coupled with good standards and policies are key steps in militating against these internal threats.

A moment of carelessness

Let's meet Barry, Claire and Sandeep, who work for the fictitious company 'Star Ex Oil.' Barry is head of IT security. He has recently overseen the roll out of a security software product across the company's business application servers. The product checks and reports on various security vulnerabilities and configuration issues. Claire also works for the IT department, as a technical trainer; she is nervously looking forward to an online training session that she is presenting later for senior business users on the subject of information security.

Sandeep is a senior computer operator who works overnight shifts. Star Ex Oil is a small firm and the overnight operators are also utilised as quasi security guards, responsible for ensuring the building doors are locked and the alarm system set on any unused floors. Each morning, around 0600hrs, they are required to permit cleaning staff to enter the building.
One morning Sandeep let a cleaner into the building who he did not recognise. The man nodded curtly and headed upstairs. Suspicious and increasingly concerned with the man's behaviour, Sandeep pleaded: 'Please just leave, please I beg you, just leave.' Then before the Police were called, the man did leave, carrying a couple of laptops and numerous confidential documents.

Claire's training session went well, the users learnt all about security best practices; the company's clear desk and social media policies. After the telephone conference had ended, Claire forgot to un-share her PC from the attendees viewing her presentation. She then proceeded to look at some pictures of a friend's new puppy sent her via email. Anybody who had not signed out of the earlier presentation was able to observe her viewing said photos. When her break was over, Claire then opened up her laptop for viewing her team's passwords file, containing generic username and passwords to various sensitive systems.

Barry was pleased when the new security software he had commissioned provided attractive looking charts and detailed server security information. In particular he was interested to read the report which listed the users identified as currently using weak or 'guessable' passwords. He took a screen-shot of the report, attaching it to an email to each user requesting they change their passwords with a stronger one. So each user now had a list of all the other users who had easily guessable passwords. Remember, no such list of accounts with guessable passwords existed until Barry, with the purest of motives, set about creating one.

Although the above names have been changed, the stories are all based on real life occurrences. None of the folks involved would have considered themselves malicious or an insider threat, but yet they performed the exact same actions that bad guys do. They created lists of vulnerable accounts, distributed sensitive password information and provided unauthorised people physical access to company IT systems.

The lesson

The lesson here is that there can be no substitute for ensuring staff awareness with regular training, having published standards and polices, and the acceptance that everyone in your organisation can represent an insider threat.

Let's finish with another question:
What are the characteristics required for a person especially suitable for working directly in the concern of information security?

Well a good eye for detail is one. Perhaps you noticed the initials of the three individuals in the Star Ex Oil scenarios spelt out BCS? But can you ascertain the brand of watch I left at Hatton Garden? The answer is there; in fact I've included it twice in the article, but just like the insider threat, it is hidden from plain view and more often than not the devil is in the detail.



Image: iStock.com/530101259

FORRESTER

Blog: Is breach notification a part of your incident response plan?
Is customer-facing breach notification and response a part of your incident response plan? It should be! This is the part where you notify people that their information has been compromised, communicate to employees and the public about what happened and set the tone for recovery. It's more art than science, with different factors that influence what and how you do the notification and response.

Unfortunately, many firms treat breach notification as an afterthought or only as a compliance obligation, missing out on an opportunity to reassure and make things right with their customers at a critical time when a breach has damaged customer trust.
7 March 2016
http://blogs.forrester.com//heidi_shey/16-03-07-is_breach_notification_a_part_of_your_incident_response_plan

Report: Four quick wins to improve security without detracting from customer experience
While many digital businesses have optimised digital customer experiences, rising customer awareness and concerns regarding security and privacy mean customers now want assurances your firm is protecting their data and using it appropriately. Unfortunately, some businesses fail to implement and demonstrate strong security measures, increasing customer attrition. This report examines the evolving balance between usability and security and how security and risk professionals can boost security without negatively affecting customer experience.
8 December 2015
https://www.forrester.com/report/Four+Quick+Wins+To+Improve+Security+Without+Detracting+From+Customer+Experience/-/E-RES123901

Predict and prevent attacks targeting the internet of things
The internet of things (IoT) is not a future trend; it is here today, and the risk of attack is real. IoT exploits are reported occurring with increasing frequency, creating a state of concern for enterprises and consumers alike. This report analyses the attributes of IoT risk by industry. The framework provided helps enterprise security and risk professionals predict when the products they are building or the technologies they use will likely become targets of attack.
7 January 2016
https://www.forrester.com/report/Secure+IoT+As+It+Advances+Through+Maturity+Phases/-/E-RES128642

GARTNER

Predicts 2016: Security for the internet of things
As the internet of things (IoT) presents an ever increasing security problem, several security areas are advancing to cope with the IoT's evolution, including network segmentation, isolation solutions and cloud-based security. IT leaders should evaluate revising strategies or purchasing new services.
https://www.gartner.com/doc/3176918/predicts--security-internet-things

OVUM

Analyst View: Privacy Shield unlikely to go ahead without further amendments
The Article 29 Working Party (the body that groups together the Data Protection Authorities of EU countries) has sent the European Commission (EC) back to the drawing board on the Privacy Shield, the agreement between the EU and the US on the transfer of personal data.

Tech companies have eagerly awaited this agreement since the demise of Safe Harbor. Luca Schiavoni, Senior Analyst, Regulations says: 'Companies affected by this agreement should prepare to face more uncertainty, because the deal is likely to undergo further amendments before it is finalised.'
13 April 2016
http://www.ovum.com/press_releases/privacy-shield-unlikely-to-go-ahead-without-further-amendments/

EBSCO articles

Mitigating cyber-threats from the inside out
Insider threats to information security continue to elude many organisations, and this article reports on how to mitigate them. A common misconception among companies is that insider threats can be mitigated merely by implementing tools or technology that can identify anomalous activity or behaviour.

The article states that one of the most important measures toward establishing a robust insider threat programme is to have clear practices and policies from the beginning, and employees' awareness of policies should also be tested. Information security is taking centre stage in many companies and more resources are being deployed to protect it.
By Jaclyn Jaeger
Source: Compliance Week, March 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=113455821&site=ehost-live&user=ns004994&password=RFq52nap

U.S. and UK firms not protecting their cyber borders
The article reports on a survey which reveals that security is not getting enough attention in organisations, for example 53 per cent of IT decision makers in the USA and the UK stated that it is easy for a former employee to log in and access data.
Source: Information Management Journal, Nov/Dec 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=110923652&site=ehost-live&user=ns004994&password=RFq52nap

At risk and unaware
This short article reports the results from a survey into UK employees' awareness of information security. Less than 30 per cent of IT workers think that other personnel are sufficiently educated about IT security. More training is needed, but employees are often frustrated by their organisation's security, with 91 per cent saying their productivity suffered as a result of their employer's approach to it.
By Stephanie Castellano
Source: TD: Talent Development, February 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=112712471&site=ehost-live&user=ns004994&password=RFq52nap

New approach for detecting leakage of internal information; using emotional recognition technology
Damage due to internal information leaks by insiders is more serious than that by outsiders because insiders have considerable knowledge of the system's identification and password, the security system, and the main location of sensitive data. Therefore, many security companies are developing internal data leak prevention techniques such as digital rights management, and system access control.

However, these techniques cannot effectively block the leaking of internal information by insiders who have a legitimate access authorisation. Therefore, the writers have switched the detection target from objects (internal information) to subjects (insiders), and concentrated on when biometrics signals change, when an insider conducts abnormal behaviour.
By Lee Ho-Jae, Park Min-Woo, Chung Tai-Myoung , Sungkyunkwan University, Republic of Korea, and Eom Jung-Ho, Daejeon University, Daejeon, Republic of Korea
Source: KSII Transactions on Internet & Information Systems, November 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=111482972&site=ehost-live&user=ns004994&password=RFq52nap

Secure communications
The article suggests that public relations and IT professionals should meet regularly to make sure they would be able to communicate effectively if there is a data breach. The writers cite data breaches that have become disastrous for the company's reputation because of lack of a careful PR strategy. The article therefore explores how to build a good relationship between IT and PR, and the resulting benefits.
By Jon M. Philipson and John E. Clabby
Source: Public Relations Tactics, September 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=110168712&site=ehost-live&user=ns004994&password=RFq52nap

10 cyber threat predictions for 2016
This article discusses some of the major cyber security risks that information security experts are watching for in 2016. They include: the spread of ransomware holding data or entire websites hostage; hackers causing more reputational damage to organisations; wearable computing devices providing a backdoor to collect data for phishing attacks; the targeting of cloud computing's vulnerable boundaries; more attacks on small and medium sized businesses; and increased hacking of critical infrastructure.
By Hilary Tuttle
Source: Risk Management, March 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=113211831&site=ehost-live&user=ns004994&password=RFq52nap

UK's National Crime Agency builds on global efforts to roll back cyber crime
The UK's National Crime Agency is making progress dealing with cybercrime through international cooperation, according to this article. An international workforce has been set up and meets on a regular basis, and seven European countries ran a cyber-attack simulation exercise in December.

The UK's campaign against cybercrime focuses on the criminals who produce and distribute malware. Education is also important with the UK aiming to make sure teenagers are aware of the havoc they cause if they get involved in a distributed denial-of-service attack.
By Warwick Ashford
Source: Computer Weekly, March 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=113988256&site=ehost-live&user=ns004994&password=RFq52nap

What EU's cyber security bill means for UK industry
The implications of the EU's first legislation on network and information security for UK companies are discussed in this article: the Network and Information Security (NIS) Directive is designed to provide high level network and information security throughout EU member states.

The directive seeks to overcome the fact that networks are not bound by geography and nationality. For companies, it dictates that operators of essential services (such as transport, health or telecommunications) must manage the risks to their networks, and ensure they have taken appropriate measures to prevent attacks and minimised their potential to succeed.
By Peter Ray Allison
Source: Computer Weekly, February 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=113988253&site=ehost-live&user=ns004994&password=RFq52nap

Every click you make
The article focuses on a proposed British surveillance law, the Investigatory Power Bill, which would allow the Home Office to track internet connection records. Documents from whistle-blower Edward Snowden suggest the government was already tracking this data and that the law would require internet service providers to keep a record of their customers' internet usage. The article speculates that the law won't be useful to catch savvy criminals, as they already use encryption, but it would harm citizen privacy and could result in pushing criminals towards using encryption.
By Jacob Aron
Source: New Scientist, November 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=110929704&site=ehost-live&user=ns004994&password=RFq52nap

Are we safe in your hands?
As cyber-attacks grow more sophisticated, the consequences if they succeed are becoming more serious. This article looks at how secure the UK energy industry is and what measures are being taken to protect it. For example, GCHQ, the Centre for Protection of National Infrastructure, and other government bodies take a particular interest in protecting the UK's energy control systems. The security around these systems is continuously re-evaluated and any suspicious activity is treated extremely seriously by the authorities.
By Dean Kelshall and Ellen Fraser
Source: Utility Week, November 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=111386387&site=ehost-live&user=ns004994&password=RFq52nap

IBM, Ponemon Say app security still lags in the enterprise
This short article discusses the findings of the study entitled 'How to make application security a strategically managed discipline' released by IBM and the Ponemon Institute. In the study 35 per cent of the respondents said that their organisations are not performing application security testing for application vulnerabilities. This is a result of developers being under pressure to deliver quickly and a huge number of apps now being deployed.
By Darryl K Taft
Source: eWeek, November 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=113756193&site=ehost-live&user=ns004994&password=RFq52nap

How to avoid the hazards of ransomware
The article gives advice on how to avoid ransomware, which is malware that prevents or limits users from accessing their system until a ransom is paid to decrypt it. Most ransomware is distributed through email, and companies can take fairly simple measures to avoid getting caught, for example through effective back-ups. Some are still getting caught out, however.
By Dan Raywood
Source: Computer Weekly, January 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=112457066&site=ehost-live&user=ns004994&password=RFq52nap

More Mac ransomware sure to surface despite halt to first attack
While the vast majority of Mac users were able to avoid the malware called KeRanger, it is not safe for them to assume that the hackers will not develop better luck and better ransomware. In the past, Mac users have not had to worry about malware because their market share was so low but, as this has increased, so has the temptation for malware writers to target it.
By Wayne Rash
Source: eWeek, March 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=113588241&site=ehost-live&user=ns004994&password=RFq52nap

Cloud security policy brings risk out of the shadows
Business leaders want to use the cloud because of its distinct advantages over what can be built in-house. Security professionals have raged against it for years but most have come to the realisation that the cloud is happening. This writer discusses what to consider when putting together a cloud security policy and some questions to ask. Cloud service providers don't usually offer details of all their security controls, but often they may have a better grip on security than most other organisations, according to the writer.
Source: Information Security, February 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=113774393&site=ehost-live&user=ns004994&password=RFq52nap

Wide disparity between consumers, IT pro views of IoT security
There is a disparity of opinion between consumers and specialists in cyber security and IT regarding the security of connected devices, according to ISACA research. The risk from the internet of things (IoT) is considered to be under-estimated and under-secured among businesses. This article lists some of the best practices suggested by the report to organisations, and for IoT manufacturers.
By Chris Preimesberger
Source: eWeek, October 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=110414361&site=ehost-live&user=ns004994&password=RFq52nap

Cloud security is a challenge for users & providers
Many cloud service providers make various security pledges, but this writer believes they should not be taken at face value. Companies must do due diligence and actually read and question cloud providers' contracts before they sign them, even though cloud providers are getting better at security. The article lists various certifications that are available for cloud service providers.
By Joe Mont
Source: Compliance Week, January 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=112087302&site=ehost-live&user=ns004994&password=RFq52nap

Bring your own risk in BYOD
Employees like the flexibility of bring your own device (BYOD) policies, but it brings risks with it. There are various enterprise mobility management solutions to help make BYOD programmes more secure. This article discusses: how centralised device management can help; how the risk landscape has changed; what security measure should be applied to BYOD; how to set up and develop a BYOD policy; and how organisations can have an oversight of the devices.
By Claire Meyer
Source: Security: Solutions for Enterprise Security Leaders, April 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=bch&AN=113913552&site=ehost-live&user=ns004994&password=RFq52nap

Quantum leap?
The impact of quantum computing on data encryption is discussed in this article. Although quantum-level computers are at least 10-20 years away, some security experts believe that preparations should be made now for quantum computers that will be able to slice their way through complex encryption algorithms. Others think that the threat it not so dire, as encryption only represents one pillar of security; key management and access control are the most common technological culprits in data breach.
By Doug Olenick
Source: SC Magazine: For IT Security Professionals, December 2015/January 2016
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=111991210&site=ehost-live&user=ns004994&password=RFq52nap

Rethinking your IT leadership strategy
The main change in IT leadership roles over the last decade has been the creation of the chief information security officer (CISO), according to the writer. She often has to question organisations as to why they are hiring a CISO. If one is really needed, she suggests it is often better to organically grow the IT team, and blend the CISO and CIO roles. This creates a healthier team and bridges the gap between CIO and CISO.
By Patricia Titus
Source: SC Magazine: For IT Security Professionals, October 2015
http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=iih&AN=109924773&site=ehost-live&user=ns004994&password=RFq52nap