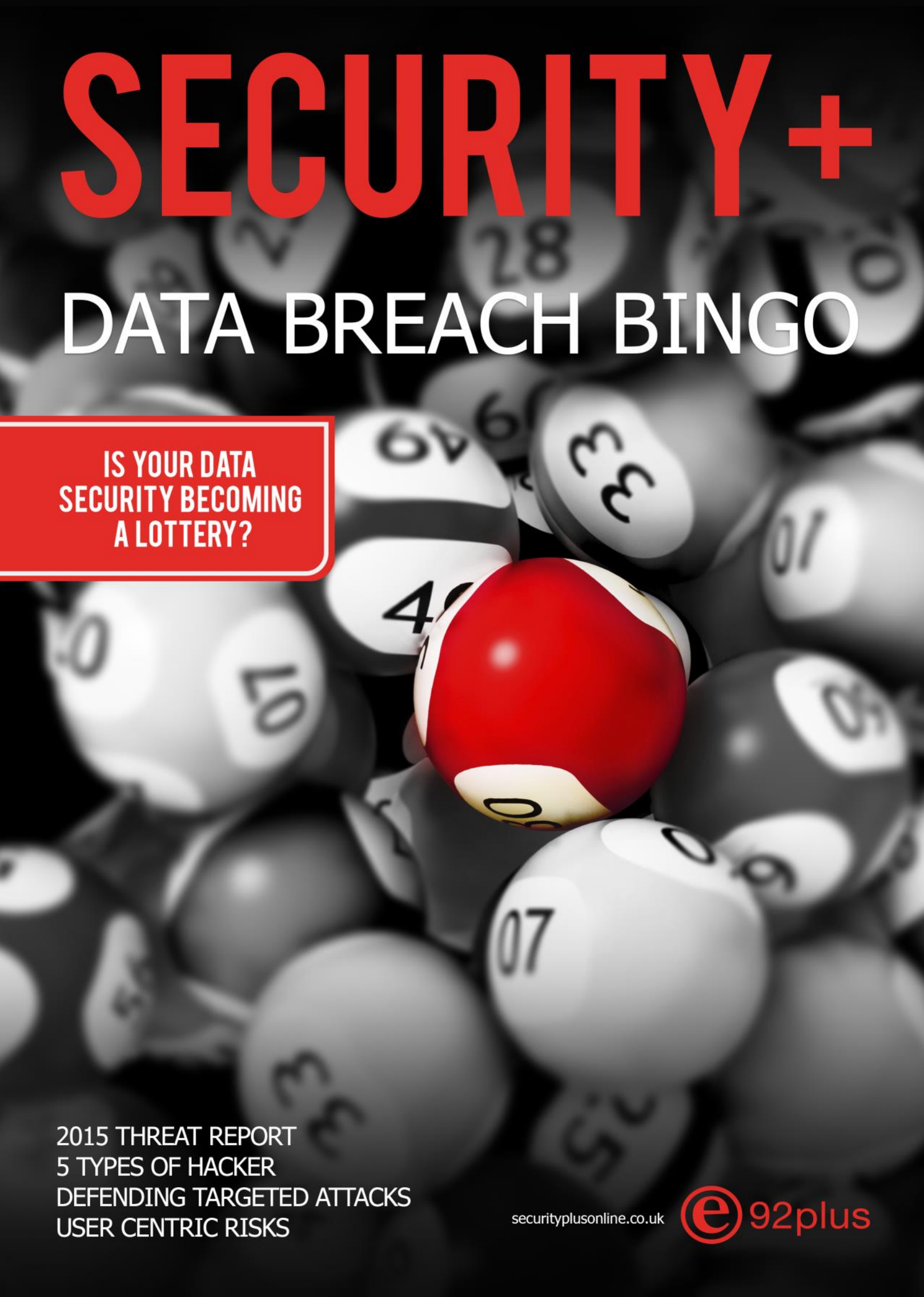
SECURITY+

DATA BREACH BINGO



IS YOUR DATA SECURITY BECOMING A LOTTERY?

2015 THREAT REPORT
5 TYPES OF HACKER
DEFENDING TARGETED ATTACKS
USER CENTRIC RISKS

securityplusonline.co.uk

e92plus

WELCOME TO THE LATEST EDITION OF SECURITY+ EXCLUSIVELY FROM E92PLUS

Essential industry insights, opinions and interviews.

Data. It's been claimed to be the new oil - but the supply is only ever increasing, and is created every day by all of us. But who owns it, is responsible for it and, most importantly, protects and secures it, is one of the biggest challenges for our industry. From social media logins for Guest Wi-Fi to sharing a confidential spreadsheet over email or a file-sharing website, the risks are increasing but IT department control is reducing. In this issue of Security+, we look at the challenges, the threats and how organisations can take back control of their data or their employees and customers - without losing productivity or mobility.

If you're interested in any of the topics or solutions featured, we'd be delighted to bring our 25 years of experience to help your organisation through our Technical Consultants, a demo or a live proof of concept.

Finally, we always appreciate feedback on Security+ magazine – so feel free to drop us a line at **securityplus@e92plus.com**. We look forward to hearing from you.

Mukesh Gupta
Managing Director of e92plus

VISIT US ONLINE

Looking for even more insight, analysis and engaging contact?

You can find more articles, resources to download and videos at **www.securityplusonline.co.uk**

GET IN TOUCH

Want to keep up with the latest industry news or just get in touch?

You can contact or follow us on

twitter.com/e92plus
linked.com/company/e92plus
www.e92plus.com
info@e92plus.com

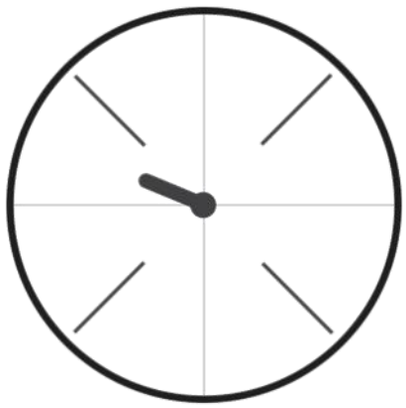
WE'RE HERE TO HELP

Our Security and Wireless Engineers have helped support thousands of organisations protect and empower their network, data and employees.

To book a FREE 30 minute security healthcheck for your organisation, register your interest at **www.e92plus.com/healthcheck**

INSIDE THIS EDITION

NOW IS THE TIME TO ACT ON CORPORATE DATA PROTECTION



The recent spate in data breaches and security threats that make global news headlines serve as a constant reminder of the need to improve monitoring and protection of corporate data. But if European businesses thought things were challenging now, then the impending changes to the EU Data Protection legislation for protecting personally identifiable information (PII) for all EU citizens – which will impose stricter fines on companies that suffer data breaches – will simply amplify that.

What the EU Regulation means

The new EU Regulation will place stronger restrictions on companies' data protection policies and systems. It will become law in each EU Member State (replacing the DPA in the UK), and further empower the Information Commissioner's Office (ICO) with the EU backing to tell companies they must take action on data protection.

The current EU Directive and UK DPA have limited effect, with organisations often happy to take the fines for suffering a data breach rather than spending the significant time, resources and funding on a data protection security programme. Indeed, at a recent financial services roundtable a number of security professionals reported that their boards do not currently feel the ICO has the power to come after them, and they are willing to accept the risk and even the maximum £500,000 penalty.

This leniency will change dramatically when the EU Regulation comes in to play when any data controller must notify the ICO within 72 hours of becoming aware they have suffered a data breach. **They could incur fines of up to 5% of their annual worldwide turnover if they are found to have been negligent in protecting the data**, not to mention the impact the disclosure will have on their brand. However, this legislation isn't simply about fining organisations. It's about encouraging organisations to become better at detecting breaches and helping security professionals be better informed to advise the boardroom of the legislation. They need to know what's being proposed so they can improve data protection and better manage or potentially increase their security budget spend with the ultimate aim of better protecting EU citizens' data.

Businesses are not prepared

Independent global research suggests that businesses are nowhere near prepared for the new regulations to come into place. **80% of the 5,000 IT security professionals surveyed explained that they believe their executives do not link data breaches to financial loss.** Whereas Ponemon Institute data estimates that the average cost per lost or stolen record from a data breach is $188, while the average cost of an organisational data breach is $5.4 million – figures that will only increase with the new regulations.

Less 50% of the IT security professionals researched felt they had a good understanding of the threat landscape facing their company. Worryingly, only a third of respondents that had suffered data breaches knew exactly what data had been stolen from them. It is therefore clear that business security is deficient; security intelligence is worryingly low and that user education levels need improvement.

Organisations that are investing heavily in monitoring, processing and managing their networks have no excuse for not protecting their data, and they need to learn to spend their security budget more appropriately with a move away from infrastructure-only security, to a modern and more successful risk-based, data-centric strategy. The threats facing companies that fall foul of the law make it even more of a necessity that everybody within an organisation is fully aware of the risk. They must build a culture within their companies whereby employees constantly consider the privacy risks that surround every process.

The rise of the DPO

The Data Protection Officer (DPO), for those organisations that have one, will have a vital role to play when the new legislation comes into force. They are fully responsible for ensuring that their organisation is aware of and complies with legislation. All too often the DPO sits on the legal team and may be unwilling to get involved or engage with the information security team. They now need to be fully aware of the technology that is being used to protect data and become part of the general security education within the organisation. To assist them in this mammoth task, they will need to define and delegate to information owners, who will act as a data protection representative across each business unit. The onus is now firmly on security professionals to ensure their organisations have robust data protection policies in place and that all staff are aware of the risks they could expose their company to.

The proposed EU Regulation allows for a two-year preparation period purely for the purpose of helping companies get better at detecting data breaches, so there is no excuse for companies that are not getting started on this immediately. To get the ball rolling, greater education on data protection for all employees, in addition to developing rigid data protection policies, is absolutely imperative over the next two years.

Neil Thacker, Information Security & Strategy Officer, Websense

websense®

2015 THREAT REPORT

Executive Summary

In this age of rapidly expanding data and highly skilled threat actors, technological advancement presents the urgent duality of great opportunity and great risk. Your data is integral to both and a key asset that differentiates your organisation. It's impractical to completely 'lock it down' and yet its open use can threaten your organisation's very existence. The challenge before security leaders is striking that delicate balance between being security aware and remaining business driven.

The human and technical aspects of cyber threats changed dramatically in 2014. In-depth research has seen new techniques blended with the old, resulting in highly evasive attacks. And while vulnerabilities were found and exploited in old infrastructure standards, developments such as the Internet of Things (IoT) have emerged to present a completely new set of infrastructure challenges.

Advice in the report ranges from the tactical to the strategic, recognising the importance of solutions that can provide specific benefits yet work as part of a unified security posture. The security recommendations provide actionable information and guidance, while taking into account the need for organisations to grow and innovate at the same time.

For executives, the report identifies key security threat trends. For IT security personnel, it helps identify the appropriate adjustments to their processes, policies and security tools needed to mitigate the risks that this year's cyber threats pose.

One particular area of risk that is a major threat to organisations of all kinds is the rising losses and costs of data theft. The report has identified eight specific threat trends that pose significant risks for data theft in 2015. These trends are reviewed across two categories to examine who is doing what and how they are doing it.

Human Behavioural Trends

- Cybercrime just got easier
- Avoid the Attribution Trap
- Elevating the IQ of IT
- Insight on the Insider

Technique-based Trends

- Building on a Brittle Infrastructure
- Something New or Déjà Vu?
- IoT: The Threat Multiplier?
- Digital Darwinism: Surviving Evolving Threats

Behind the Report

The Websense ThreatSeeker Intelligence Cloud was a primary source of data for this report, receiving up to 5 billion inputs daily from around the world. Expert interpretation was provided by Websense Security Labs based on interviews and investigations performed by researchers in Europe, the Middle East, Asia Pacific and North America. As both researchers and engineers, with full Kill Chain analysis expertise, threat information was interpreted with respect to the overall context of attack activity and the potential impact for any operational systems affected. As a result, threat trend information is provided in four areas:

- **Overview –** What is the observed trend?
- **Evidence –** What data or behaviour was seen?
- **Impact –** What is the risk if not addressed?
- **Guidance –** Actionable recommendations for consideration.

In Conclusion

In 2015, simple adjustments to security solutions will not meet the challenge. Your holistic security posture must be re-evaluated in terms of both human and technical elements. Supportive tactics will require adaptive security solutions. The risk from the human elements of security has grown on both sides of the battle. On the one hand, threat actors are increasing both in skill level and in sheer numbers. On the other, the on-going shortage of highly skilled personnel will require investments in IT, in people, education and tools to maximise their effectiveness.

The techniques displayed by the latest cyber threats have shown innovative improvements in evasion and the blending of old school tactics into modern attacks with devastating consequences. At the same time, threat actors discovered how to exploit legacy infrastructure vulnerabilities in new ways. No doubt we will all see more of the same going forward. And, the emergence of the Internet of Things will only add more vectors for entry and compromise for threat actors to use against unprepared networks.

Download a full copy of the 2015 Threat Report today

Register now to gain executive visibility of key security trends and specific guidance in optimising processes, policies and security tool usage. You will also get access to the recorded webcast events, with our security experts discussing the impact and future implications of these trends and threats.

Visit www.websense.com/2015threatreport today for more information and your free copy of the full report.

"Do not underestimate the risk of the motivated malicious insider. Those with access and intent are considered to be just as dangerous, if not more so, than external threat actors."

Carl Leonard, Principal Security Analyst , Websense Security Labs

Exclusive Extract: Something New or Deja Vu?

What's old is new again. Tactics from the 1990s, such as malicious macros in unwanted emails, will continue to be "recycled" into new threats and launched through email and web channels. Threat actors are blending these old tactics with new evasion techniques, new exploits and more to create threats that challenge even the most robust defensive posture.

Recycling social engineering messages is not new but 2014 saw growth in recycling other tactics, blended with new methods and techniques for improved evasiveness. One example of this renaissance of threat tactics, measured by Websense Security Labs, identified over three million macro-embedded email attachments in just the last 30 days of 2014.

A good example of the effectiveness of this approach was demonstrated mid-year, when a very modern, targeted and otherwise advanced attack on the financial sector used Microsoft Word macros that were extremely adept at evading detection. It should not be overlooked that email, the leading attack vector over a decade ago, remains a very potent vehicle for threat delivery despite the now dominant role of the Web in cyberattacks.

In 2014, 81% of all email scanned by Websense was identified as unwanted - up 25% from 2013. What's more interesting, beyond the volume of malicious emails, is the fact that Websense detected 28% of malicious email messages before an anti-virus signature became available, presenting AV users with an average window of exposure of 17.5 hours. These figures underscore the importance of employing real-time scanning and protection against the sizeable quantity of rapidly iterating malicious material.

A Case Study

One particular attack targeted fewer than 100 accountants in the financial services sector for their valuable data, using a blend of techniques that took advantage of their daily reliance and familiarity with macros within documents and spreadsheets. A message was socially engineered for the victims, leading them to open the attached Microsoft Word document and then to run the macros.

Once they did this, the macro contacted a website to download an executable that opened a backdoor into the machine to progress the attack through the Kill Chain. A second round of the campaign occurred one day later, with different attributes (i.e. sender and subject).

BATTLE STUDIES

THE IT SECURITY VETERAN'S STEP BY STEP GUIDE TO KEEPING YOUR NETWORK SAFE

Security is paramount to any wireless network. Not only being compliant but protecting your information is vital in an age where targeted attacks are evolving, leaving network security providers having to stay ahead of the game. Any technology section of any online news publication will have covered some of the IT Security horror stories from the last 12 months. Sony, CNN, Anthem, Chick-fil-A, U.S. Postal Service, Microsoft, Staples and JP Morgan are just some of the big names that have been victims of some form of cyber-attack in recent months.

But what often goes unreported is the number of small and medium sized enterprises also falling foul to the exploits of hackers. 60% of small UK businesses experienced a cyber-security breach in 2013, with a similar percentage in 2014. Companies simply cannot afford to skip or overlook the essentials regarding the security of their network. Protection and detection is a must and taking the right steps is important.

1. The Internet of Things. Choose your wireless network carefully.

According to IDC, the growing global Internet of Things (IoT) market is on course to hit $7.1 trillion by 2020. With the rapid rise of connected devices in the IoT landscape there is growing concern about elevated security risks associated with the sheer volume of new devices coming online.

The design of your wireless LAN (WLAN) must plan for IoT capacity and network traffic, as well as optimal secure coverage across your site. Tracking and monitoring devices on your network as well as devices around your network are important considerations of WLAN design. Choosing the right cloud solution is imperative as the wrong solution will quickly create two scalability challenges:

1. System scalability
2. Operational scalability

System Scalability involves the ability to monitor many devices, store and process their data in the cloud whereas operational scalability focuses on minimising false alarms resulting from the exponentially increasing volume of devices on your wireless network.

Cloud Wi-Fi is a great choice to consider when planning your wireless network's ability to handle the coming tidal wave of IoT devices. On the road to an IoT future your focus should be on how your wireless network offers simplicity, scalability, and security.

The Cloud provides an optimal architecture for managing scalability especially in a large distributed environment where IT staffing can be limited.

2. Compliance. A must have, but it does not mean you're protected.

The Payment Card Industry Security Standards Council (PCI SSC) has recognised that unauthorised or insecure Wi-Fi presents a danger to network security, and as such has published wireless security guidelines to protect sensitive payment card data from wireless threats. Though PCI DSS suggests quarterly wireless vulnerability scans, a merchant can be held liable if the cardholder data is compromised in the duration between scans. The only way to guarantee a secure and compliant network requires 24x7 scanning of your wired and wireless environment as an essential step in securing the cardholder data and a recommended best practice.

In the context of PCI, compliance is adherence by all organisations processing payment card data to the minimum security requirements defined in the PCI DSS. Compliance standards such as PCI DSS set the benchmark usually for a specific industry vertical, but are not necessarily comprehensive when it comes to network and data security. On the other hand, security is the level of protection against risk. Meeting compliance requirements should not be mistaken as a certification of ultimate security

3. Living in a material world

Wi-Fi has become a transformational retail engagement platform where virtual and physical shopping experiences meet. This evolution is creating profound changes in the way retailers communicate and engage with their customers. As evidenced recently by massive security breaches at

several major retail organisations, good reputations and consumer confidence cultivated over many years can be wiped out in an instant if customer financial and personal data have been compromised.

A key component of any good retail security strategy should be the implementation of a wireless intrusion prevention system that can effectively detect and block wireless threats before they can cause any harm — preferably one that can operate autonomously 24/7 without the risk of false negative and false positive readings that could result in undesirable outcomes.

4. Threat analysis. The corporate network trap.

Some organisations aren't worried about their corporate Wi-Fi, as their policy is only to let corporate devices on to the network so that they have full control over who has access.

However, most users do not comprehend the associated risks. The invisible radio waves used for transmission make the traditional "harden-the-network-perimeter" security approach obsolete. Radio waves often spill beyond the confines of a building. Malicious hackers in the airspace can use these waves to enter your network and steal sensitive data.

This means that even a single wireless device on your premises, let alone a wireless LAN, can open a wireless backdoor to your corporate backbone network that is otherwise protected by non-wireless firewalls and intrusion detection systems. This doesn't have to be a corporate device such as a laptop; this could easily be a wireless printer that someone has gained access to, thus access to the entire network. Do not fall into the trap of thinking that only allowing corporate laptops access means you aren't vulnerable to attack.

5. Planning for the future

Security is imperative, as is planning. Remember to plan for IoT capacity and network traffic and make sure you have optimal secure coverage across your site. Too many organisations are underprepared and do not execute the proper planning. Don't be one of them, choose your network carefully.

In the end, make sure whatever WLAN you choose gives you the ability to provide an instantaneous, positive user experience that will meet the expectations of your business and customers, without compromising your security.

THE COST OF REMEDIATION

The Impact of a Cyber-Attack

31 DAYS

Average Remediation Timeframe

Cost Per Day

Total Price Tag for a Data Breach

47% of restaurants are planning Wi-Fi upgrades for mobile POS

40% of participants deemed free Wi-Fi an important or very important facility in a restaurant

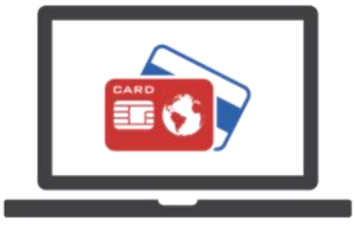
Yet 69% of consumers are **less likely to shop at an organisation** that has been breached

How does a cost from a breach typically add up?

- Reputation and brand damage
- Lost productivity
- Lost Revenue
- Forensics
- Technical support
- Compliance Regulatory

AirTight NETWORKS

FINDING THE RIGHT SOLUTION IN WI-FI MARKETING



Who hasn't spent £5 on a coffee just to have the opportunity to sit down and catch up on email or social media? Or even specifically chosen a Wi-Fi equipped café, pub or restaurant for a business meeting so that they could be sure to have a reliable wireless connection? This probably sounds familiar to many of us. Wi-Fi has become a gratuitous motivation for small businesses around the world to attract customers even though the moment the customer leaves the building, there is nothing to trace that they were ever there.

Wi-Fi is no longer a simple amenity

The customer generating power of data availability has a majority of local corner shops in shackles. Without missing a beat, entrepreneurs from around the world have jumped at a chance to monetise on this dependency, creating start-ups that promise data collection and Facebook likes. Too good to be true? Are the offers on the market matching up to business revenue objectives and client needs? And where do subjects like security, privacy and performance fit into the mix?

The Wi-Fi marketing mix

For marketers, this is a whole new way of gaining customer data and performing analytics to reach out to these users post-event; but it's also much more than that. The ability to reach out to an audience in-session and provide information to help them plan their next purchase or action is incredibly powerful. The post-event information remains vital, but the real-time delivery is a game-changer. The interesting part of this puzzle is that the choice of wireless network is no longer limited IT departments but opened up to digital marketing, data analysts and even the managerial suite. There is a lot to be gained and a decision made singularly by any one business unit is too limited and limiting.

Now, let's back up and take a look at business needs. In our coffee drinking café, the business owner's objective is likely to be to increase fidelity and target new customers. With such a Wi-Fi hungry crowd, this is a stellar opportunity to touch the audience directly through their network connection. The addition of advertisements with a free connection is a great way for business owners to get a return on investment or push other clients to opt for a paid Wi-Fi access for their browsing hours.

Varied needs for industries

The needs of different industries vary greatly however and this simple formula is turned on its head if we take the example of a hotel chain. Here, the needs of internet connection may stretch much further. Just think about the different target groups you have in a hotel: the reception, restaurant, bar, spa and rooms all demand specific marketing objectives. Beyond list creation, the clients in the bar benefit from a social login option but also a special promo to come back for happy hour, the customers in their rooms need automatic login (details already synched with the PMS system in place), higher bandwidth to allow connection to video

streaming and an eConcierge service that will affiliate the hotel with local commerce and services. This is a much more complicated equation that is rare to find in a single tool.

Similarly, a stadium owner not only needs to understand the fan demographics and provide different Wi-Fi packages (free and high bandwidth paying options), but wants to direct fans to the website where they can buy tickets for the next match or purchase T-shirts at a special rate. This can be particularly difficult when zones, such as special VIP or press access zones, are implicated. While some stadium owners are hard at work developing expensive customised Apps, the right Wi-Fi monetisation tool can provide an in-browser App with zero development needed.

Underlying needs for all business

Apart from different marketing needs, across all verticals, business owners agree that security is imperative. Given the choice, all of them want to have proprietary retention of their user information. None want to have to change a network that is already in place to start from scratch with new access points. Often, a business may find a best-fit product just to expand the business a year later and outgrow the chosen solution.

Many simple solutions on the market may appeal to café owners, but don't have the backbone to deal with security problems that could be encountered while providing free wireless access. Others may use a product that comes packaged with their access points only to find that they are severely limited in the very push marketing options that would serve them best. Large venues struggle to find a marketing tool with compatibility to their high-performance wireless infrastructure needs.
With the needs outlined above and the demands stipulated by business owners, there are, in reality, very few solutions that can run the gamut of security functions and also tie in the in-session marketing and data analytics. The truth is that you need an organic, solid foundation that is not available through most of the new offers on the market.

In summary, just type "Wi-Fi Marketing" in Google and you'll see that choices today are in no way limited. The crux is to find the solid and reliable foundation to provide security and fine-tuning while also taking advantage of the real-time push marketing and analytics that turn into ROI. This combination may just prove to be the holy grail of Wi-Fi Marketing for small and large business alike.

FROM WIRED TO WIRELESS
SECURITY BEST PRACTICES

Mobility is now an integral part of doing business. Employees, clients, and customers expect to connect without wires. In fact they are depending on it. The explosion of smartphones and tablets brought into the workplace has seen to that. Smart enterprises understand where this is heading. Wireless networking is overtaking conventional wired.

When a customer's wireless network is as reliable as wired, mobility enables workflow to accelerate. When a wireless solution is designed to handle critical applications flawlessly, productivity improves. And when wireless rich-media streaming is delivered in dense user environments, satisfaction rises. Wireless isn't a "nice to have" anymore. Executed properly, it is a strategic IT infrastructure advantage that fuels enterprises and lets you do more than ever before.

At the centre of this should be a key area: Security. With the influx of tablets, smartphones, and BYOD (Bring Your Own Device), wireless has quickly become the new norm for network connectivity. The days of network security being dependent on a directory server profile are over.

The security considerations of operating wired networks and clients are well known. Ubiquitous wireless networks on the other hand are newer to many IT administrators and so are the aspects of operating these networks. Shortcomings in the initial Wi-Fi standards tainted the perception of wireless security, but these limitations were solved with the 802.11i advancements put in place in 2004, paving the way for the broad adoption of wireless networks in all types of applications. In the end, both wired and wireless media are able to provide strong security if deployed correctly.

Wired network security, perimeter security, is based on the principle that communications are contained within the network (cables), and as long as only authorised users have access to that media, communications are secure. Wireless network security is fundamentally different because wireless communication propagation cannot be completely contained within a specific physical area, and as a result, additional security measures are required. These include user authentication, encryption of the communication, and RF monitoring of the environment.

Building a wireless infrastructure that not only meets connectivity and performance requirements but also addresses security concerns is attainable by focusing on some key best practices.

User access control

Network users, whether employees, contractors, or guests may all require network access, however each class of user should be restricted by policy to the resources that they can access, when they can access it, how much they can access.

Secured communications

Wireless communication propagates beyond the physical boundaries of an organisation; as such there is no way to restrict access to the physical medium. Wireless communication not intended for public distribution requires encryption services able to protect the data without degrading network performance.

Threat monitoring

While wireless solutions improve access and productivity, their ubiquitous coverage also enables the potential for nonconforming or even malicious devices to be deployed within the network, having the potential to impact network operation. You need the ability to identify and classify users, securely protect data as it travels through the network, and also monitor the surrounding RF environment for threats.

In short, no single device, feature, or protocol can protect your wireless or even wired network. It will always require a layered approach.

THE FIVE MOST COMMON TYPES OF MALICIOUS HACKERS

"So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss.
If you only know yourself, but not your opponent, you may win or may lose.
If you know neither yourself nor your enemy, you will always endanger yourself"
- Sun Tzu

A few years ago, we looked at the five main archetypes of a hacker. While in many circles "hacker" has become a catchall name for 'bad guys' perpetrating cybercrimes, it's important to note that not all hackers wear black hats and commit criminal acts. Some hack to test product vulnerabilities and improve overall security. Hacking encompasses a whole culture and not all hacking is done with computers. However, there are different types of hackers with varying motivations. Knowing more about malicious hacker archetypes and their particular intent can help security solution providers tailor their tools more effectively and can help an organisation plan a more advantageous defence.

We took a look at the world of malicious hackers to see if the five main archetypes we previously identified remain the same now, or if the world of illicit hackers has changed (and how) over the past few years. We found an evolution of hackers with similar designs, as well as new and sophisticated tools. Present-day hackers fall into categories you can see opposite.

While all of this discussion of hacker types and sorting out the bad apples can make for an interesting read, it will provide no solace if you or your organisation becomes a victim. However, by understanding the most common motivations and archetypes of the cybercriminal underground, we can better defend ourselves from their attacks.

Carl Leonard, Principal Security Analyst ,
Websense Security Labs

THE ARMS DEALER

Who: The "Arms Dealer" is a hacker who develops and sells malware and other hacking tools and exploit kits to other cybercriminals. The 'Arms Dealer' might also specialize in "ransomware" or be renting out botnets or selling Trojan toolkits, keyloggers and other malware on the black market.

Why: Arms Dealers can make good money on underground markets simply by selling their toolkits or renting out access to zombie computers (so called for performing malicious tasks under remote direction). They can quickly and easily modify their malware and sell new versions when antivirus and antimalware security tools shut down the old versions.

Example: The infamous Zeus Trojan has been sold on the black market for several years now. Perhaps the most successful Arms Dealer of all time is "Paunch" who created the Black Hole exploit kit, changing the face of the cybercriminal arms industry by offering frequently updated packages, hosted services and criminal infrastructure, including obfuscation modules, as a service.

THE BANKER

Who: "The Banker" is highly focused on stealing credit details, PII and other information including username/password credentials that can be sold and traded on the black market. These hackers are often based in China, Russia or Eastern Europe. They may use phishing attacks to capture user credentials, or employ advanced malware to steal valuable data.

Why: Once these hackers steal credit card information or other valuable data, they treat it like any other commodity that can be sold or traded. Rather than use the data to commit identity theft or make fraudulent purchases themselves, they sell the information on online underground markets for a tidy profit. The information is then used by many more hackers and crooks in a variety of crimes.

Example: The massive breach at Target Corporation where hackers stole information of more than 40 million credit and debit cards in late 2013. Hackers used malware to compromise Target's point-of-sale registers and capture the card information. It's reported that as many as 3 million stolen cards were sold on the black market in the days after the breach. The hackers are estimated to have made more than $53 million from the sale of the credit card information.

THE CONTRACTOR FOR HIRE

Who: Teams of hackers who rent out their services. Often residing in China, Russia or Eastern Europe, these hackers for hire can be one or two individuals; or part of a larger, organised crime syndicate. They possess a variety of skills necessary for breaching networks and stealing data, often using phishing attacks and Trojans. It's a well-established industry and their services can often start at just a few hundred dollars.

Why: These contractors are often hired to target specific organisations or to steal specific types of information such as credit card information or passwords. They are sometimes even hired for state-sponsored espionage. Hackers for hire are in it for the money and they will target organisations of all sizes and in all industries, depending upon what they've been hired to do.

Example: In early 2014, the FBI arrested five individuals for running the "hackers for hire" website needapassword.com, which promised to provide paying clients with stolen passwords. The group charged customers anywhere from $50 to $350 for passwords.

THE SPECIAL AGENT

Who: These individuals deal in highly-targeted, advanced persistent threats (APT) and cyber espionage. They may be a state-sponsored agent of a foreign government or even a source within an organisation working as a double agent. These types of attacks are costly, time-consuming and sophisticated, focusing on very high-value targets such as large corporations in the finance, IT, defence and energy sectors.

Why: The Agent is in it for cash, creed or country. They typically are looking to steal trade secrets, financial data or strategically important information on energy and defence systems. They may conduct covert, on-going spying campaigns, or they may overtly disrupt business and sabotage organisations or public infrastructure.

Example: In 2014 US federal agents notified more than 3,000 US companies that their computer systems had been hacked. The estimated cost of these targeted attacks against US companies is up to $100 billion annually. A hacking organisation called Hidden Lynx was also uncovered and alleged to have been commissioned by the Chinese military for cyber espionage campaigns, and linked to several notorious attacks including Operation Aurora which targeted Google and Adobe among others.

THE ONLINE ANARCHIST

Who: A loosely organised group of underground hackers and pranksters, mostly seeking to cause chaos for organisations or people they dislike, or provide support for the causes they follow. They often launch DDOS attacks, or deface a company's website to cause embarrassment or to disrupt the company's activities.

Why: Many hackers in this group started off as independent script-kiddies testing their skills in one-off battles, public forums and boards such as reddit and 4chan, allowing them to find a community and a cause to unite around. As a loosely-defined group, this hacker archetype comprises individuals with varying motives, from those conducting online political protests to those simply acting as hooligans out to cause mischief.

Example: The group calling itself Anonymous and its subgroups LulzSec and AntiSec are the most well known examples, gaining notoriety in 2008 with high profile attacks. Recently, the Syrian Electronic Army (SEA) took over the homepages of eBay and PayPal in the UK, France and Israel. Rather than stealing data, they promoted their cause, saying the attack was in retaliation to eBay's and PayPal's lack of presence in Syria.

TREND MICRO™

Trend Micro™ Deep Discovery

TOP SCORE in Breach Detection

See why Deep Discovery earned NSS Labs coveted RECOMMENDED rating:

- **Breach detection**—99.1%, the highest of all products tested
- **Zero false positives**—none occurred during the tests
- **Low TCO**—over 25% lower than the average
- **1 Gbps Certified throughput**—100% capacity rating in NSS Labs' real-world test loads

Learn more at **www.trendmicro.com/NSSLabsTopScore**

99.1%

NSS Labs 2014 Breach Detection Tests

First came the data breaches. Then came the string of high profile resignations. Now reports are beginning to piece together the financial impact of the cyber attacks on Sony, Target, JPMorgan and others. The Japanese electronics giant has already spent $15m on remediation and is facing multiple employee law suits, while Target recently revealed a $162m hit and security experts believe losses could increase to as much as $1bn after legal costs.

If nothing else, these doom-laden headlines should help impress upon enterprise leaders the importance of information security. But without business literate CISOs to report into the board and co-ordinate a risk-based approach to securing sensitive data, there'll be no shortage of corporate cautionary tales to read about in the future.

The Target breach, like countless before it and many more after, was a classic targeted attack. The modus operandi varies slightly from breach to breach but usually involves the covert theft of valuable corporate information – in this case customer card and personal data – in order to sell on to the highest bidder or monetise some other way.

A business literate CISO to prevent the next Target-Sized Breach

By Bharat Mistry, Cyber Security Consultant at Trend Micro

Target's first failure was not to have a dedicated CISO in charge. It was a mistake that ultimately cost the CEO and CIO their jobs. Now rectified, it's come at a heavy cost to public and investor confidence in the company. We've also heard that JPMorgan had only just appointed a dedicated chief security officer at the time it was breached in a major cyber attack. Home Depot – another US retailer hit last year – is also reported to have struggled with a high turnover of staff in its information security division.

Board vs IT

Having a CISO in place doesn't preclude an organisation from being breached – it's merely the most obvious indicator that the board doesn't take security seriously enough. By security here I'm talking about the umbrella term of "information security" – the protection of key business data – rather than "IT security", which could be interpreted as the more technical discipline of locking down IT systems against attack.

If a CISO is in place but is marginalised and/or can't speak the language of the business then there's still a high probability that the organisation in question will suffer some form of successful cyber attack or data loss incident. These occur because the tech side sees security as an IT issue and not a business risk which needs articulating to the board. I talk to countless IT leaders who complain security budgets are reducing. But that's happening because they're not explaining well enough the importance of their function to the business.

So what happens is mutual ignorance – the board doesn't appreciate the value of info-security and IT doesn't get what the business is doing.

The problem historically has been that business leaders operate according to risk – they take risks to gain a competitive advantage. On the other side the IT team is risk averse, which is why it's so often seen as a block on productivity, business agility and growth. It's why, for example, we've seen "shadow IT" spring up in so many organisations all over the globe, as normal users look for ways to circumvent what they see as over-rigorous, productivity-sapping IT controls.

Say it with metrics

So what can the ambitious CISO do to better communicate with the board, secure that funding and help prevent another Target? Devising a metrics dashboard is a great place to start. These are commonly used by executives to understand the spend, risk exposure and operational efficiency of projects as they progress. Done well, they can help the CISO present to the board a de facto balance sheet for the security function – outlining where spending is lagging and where investments need to be focused.

The key is to take a risk-based approach. The sheer volume and sophistication of today's threats means that you can't protect the organisation from everything. So it's up to the CISO to evaluate where the key assets lie, attach a value to them and calculate how much it would cost the business if they were compromised. That's the kind of language that the business can understand. It's the people and process side of information security rather than the technology we're often so fixated on.

This isn't to say that the technology itself should be ignored. A great way to test how fit defences are for purpose is to implement a "red team" testing initiative. Work with HR to define suitable parameters and then authorise a trusted team of white hat hackers to stress test your entire environment. The bolder the better – think targeted attacks and attempts to gain physical entry to the building. Data from this kind of exercise can feed back into that all-important metrics dashboard.

The bottom line is that data breach costs are growing – by over 30% globally from 2013 to 2014, according to PwC. Even in Europe, where the costs associated with follow-up litigation have historically been less pronounced than in the States, things are changing with new breach laws coming which could fine transgressors up to 5% of global turnover. If you haven't got one already, it's time to appoint a CISO that understands the business. The next challenge, of course, will be finding one.

SHADOW IT

THE NEW REALITY OF THE CORPORATE NETWORK

For organisations, the challenge of protecting data has become more complex with the proliferation of computing platforms, services, and applications. Where securing data used to be a vertical problem it is now also horizontal.

The perimeter is no more

Before, organisations could protect data by applying layers of security functionality to relatively static endpoints. The datacentre contained racks of servers containing data. Setting-up a new server took weeks, if-not months, from scoping, procuring, setting-up, and installing hardware, to standing-up new applications. The lengthy process involved many checks and balances. End-user systems were outside of the datacentre, but still behind hefty perimeter security. Security was concentrated at the perimeter, with layers of security down to each endpoint.

In these relatively static environments, the focus of security was adding more layers of security functionality from perimeter endpoint, and within the endpoint. This was feasible since all endpoints were owned, ordered, and deployed by corporate decree. Predictable environments were well-suited for predictable security.

Two technologies have changed everything: virtualisation and mobile computing.

As end-user computing power has become smaller and less expensive, computing has moved outside of the confines of corporate datacentre. The first cracks in perimeter-centric security appeared with the wide adoption of laptops. Mobile devices (smart phones, tablets) have exacerbated the crumbling of corporate perimeter security. End-users now often own personal laptops, desktops, and mobiles.

Virtualisation, specifically x86 virtualisation, has revolutionised how corporate datacentres are designed, built, and operated. That technology has also driven changes in end-user computing. Virtualisation powers public cloud, and working hand-in-hand with evermore powerful mobile devices, powers the delivery of an astounding variety of services and applications that are outside of corporate control.

From the perspective of corporate IT security teams, this has changed the nature of the challenge from vertical (secure highly controlled and well-defined devices running applications inside a corporate perimeter) to horizontal (secure myriad, barely controlled devices running undefined applications anywhere in the world, without forgetting about assets that are still in the datacentre).

The new security challenge is horizontal

The horizontal stretch provides end-users many options, and those end-users include application developers. For example, if corporate IT cannot provide a solution for transferring large files, end-users will use something like DropBox. If IT cannot spin-up servers for developing, testing, and launching a new application quickly, developers can virtually swipe a credit card and have servers running on platforms like Amazon Web Services in minutes. Collectively known as *shadow IT,* these applications and services are often outside of corporate control. While one is end-user computing and the other servers, the result is the same; devices, platforms, and applications that corporate IT can either compete with, embrace, or (futilely) attempt to block – which is roughly the same as trying to ignore the bully who's eating your lunch.

From a security perspective, this stretches what was once a singular risk profile – a corporate perimeter bristling with defences – across many devices and platforms. For example, Edward Snowden revealed that Communications Security Establishment Canada (CSEC), as reported by CBC, "used information from the free internet service at a major Canadian airport to track the wireless devices of thousands of ordinary airline passengers for days after they left the terminal." What about the ubiquitous free charging stands that happily accept USB connections from mobile devices? Are the free applications that users install well-behaved? Are corporate applications launched on public cloud properly secured? Is it safe to trust services with corporate data, or might there be another DropBox failure that exposes sensitive data to the world at large?

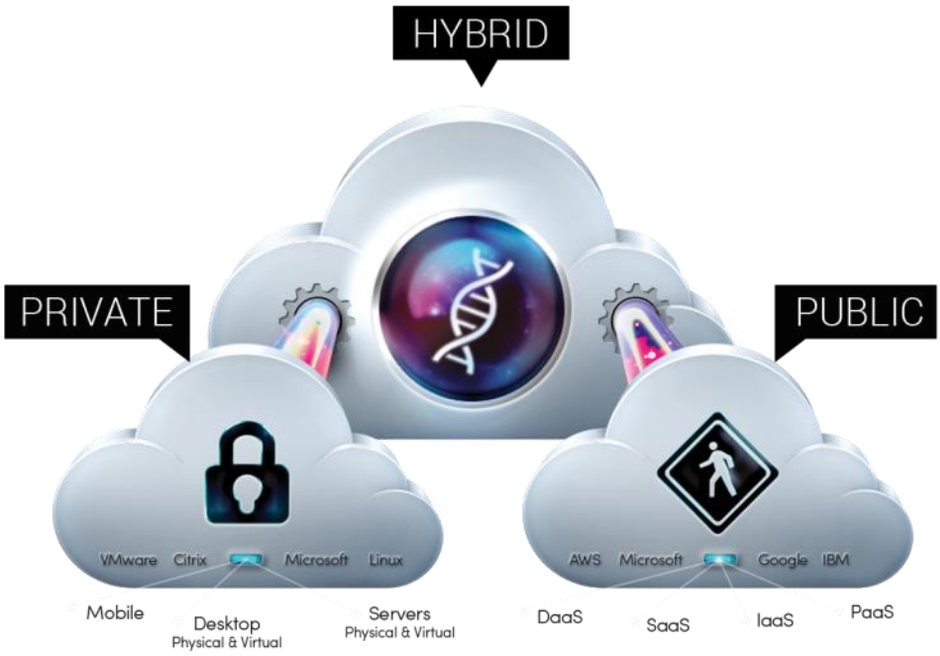
The beginning of new security is at the end of old

It is obvious that security needs to keep-up. The bad news is traditional security, built for inside-versus-outside paradigms, is failing. The good news is there are many new opportunities for security.

End-users now demand access to corporate data from anywhere. Virtualisation, specifically Virtual Desktops (whether in the datacentre or hosted) allow organisations to keep data centralised, while allowing end-users to view and work from anywhere. Companies like Citrix are focusing on enabling this via XenDesktop while Amazon has launched Workspaces, a desktop-as-a-service offering. Rather than moving corporate data to an endpoint to work with it, end-users can access data that remains in a datacentre.

Organisations that adopt service-provider strategies can also benefit. Indeed, it can be argued that continuous delivery of small incremental changes in applications leads to better application security. Likewise, it would be difficult for almost any organisation to compete with the level of infrastructure security and compliance Amazon offers.

Within corporate datacentres, endpoint security solutions have been developed by security companies like Bitdefender to optimise performance, while also being capable of delivering security in public cloud environments like Amazon Web Services.



The key to meeting the challenge of securing horizontal, highly dynamic, and widely dispersed infrastructures (for every endpoint that accesses corporate data is a part of the estate) is leveraging technology, processes, and ideologies that approach the concept of *corporate IT assets* from a new perspective.

Start by baking security into the recipe

The reality is end-users and application developers don't use shadow IT because they want to avoid corporate IT; they use it because they have to. Rather than futilely trying to cut-off end-users from data, figure-out how to provide access safely. By leveraging technologies like virtualised desktops, productivity will increase, just as it did when laptops gained wide adoption and Blackberry attached email to our hips. Likewise, if developers need servers spun-up in minutes, not days or weeks, work to meet their needs, whether through private cloud, public cloud, or a hybrid of the two. Remember – corporate IT is no longer the sole arbiter of what end-users can do; corporate IT is in competition with shadow IT.

When focusing on building services for end-users, security must be integral to the services. If the operations side of corporate IT can spin-up a server in minutes, but the security team takes days to push intrusive security before the systems are accessible, end-users will be forced to use shadow IT.

In datacentres and public cloud, this means baking endpoint security into templates. It means having a security management console that is synchronised with the ever-changing environment.

Virtual instances of desktops and servers may be spun-up and deleted at a rapid pace. If security teams are not using management tools that integrate with infrastructure management tools like VMware vCenter, Citrix XenServer, or Amazon Web Services APIs, they will be left behind.

Security must also follow the data. Developers will rapidly create new applications in corporate and public cloud datacentres, end-users will access that data from a variety of devices, and security must be present throughout.

Many points do not make a line

In trying to solve the problem of horizontal security, organisations may be tempted to add point solutions for each *new* part of the puzzle. Perhaps a traditional endpoint security solution is deployed on laptops, desktops, and servers. As mobile devices proliferate, another point-solution is acquired. As the datacentre is virtualised, another point solution is leveraged. As public cloud is adopted, yet another point solution is bought. Soon, management console exhaustion is reached – the point at which a security team can no longer maintain effective insight and control across disparate management consoles.

To solve this security management problem, look again to solutions that embrace the tenets of cloud and virtualisation. No longer is necessary to have a management console that is installed on a Windows server and tied to a SQL database. For example, Bitdefender GravityZone is a self-contained elastic management cloud. It's composed of a single Linux-based virtual appliance that can be cloned as needed, with each clone playing one or more roles in the management architecture (web management console, MongoDB database, load balancer, etc.). A single management deployment can be contained in one virtual appliance, or spread across tens, hundreds, or thousands in multiple datacentres around the globe, managing security across virtualised, mobile, and traditional endpoints.

Wrapping-up the cloud of it all

It is not a security industry secret that attackers, whether private, government, nuisance, or for-profit, are leveraging every resource at their disposal, and getting very, very good at what they do. It may be tempting to be lulled toward complacency, but that feeling will instantly evaporate when it's your name in the headlines.

It may feel as though end-users are doing everything they can to spread corporate data across the globe, but the reality is that they are taking advantage of shadow IT not because they want to bypass corporate security, but because they feel they must to meet productivity demands.

Rather than viewing developments like mobile devices, public cloud computing, and virtualisation as barriers to traditional security, view them as opportunities for facilitating the delivery of services to end-users that must be secured in new ways. Above all, these present opportunities for organisations to shed security that was "good enough" ten years ago, and move toward security solutions that are not bolted-on after-the-fact, but instead, built to defeat today's threats, drive performance across horizontal infrastructures, and deliver insight and control wherever data moves or rests.

Shaun Donaldson, Director of Alliances at Bitdefender

USER-CENTRIC RISK

WHAT ARE THE BIGGEST THREATS TO ENDPOINT SECURITY?

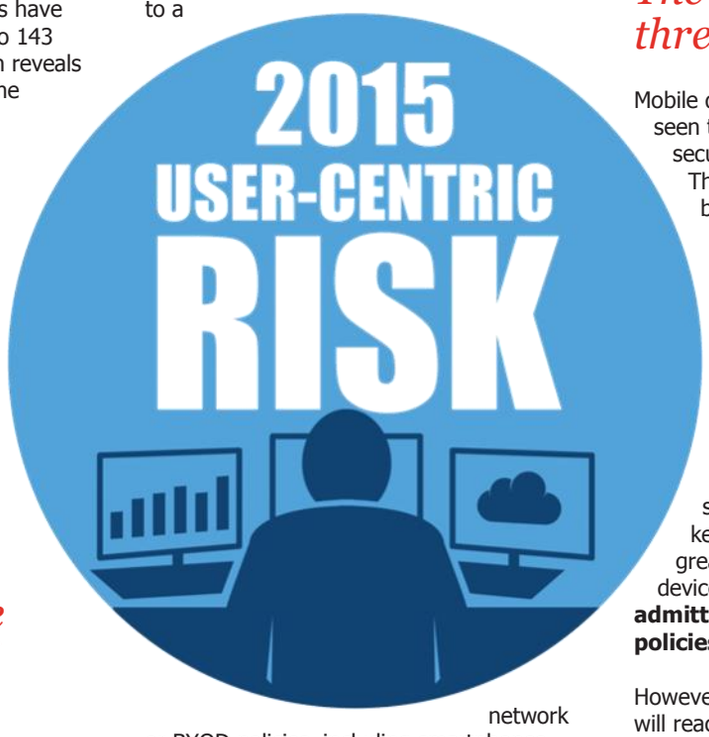
Alan Bentley, SVP Worldwide Sales at HEAT Software

Research conducted in 2015 by the Ponemon Institute and HEAT Software (formerly Lumension) has identified the user as the most significant security problem for businesses. Attacks against the user are more sophisticated, determined and persistent while malware has increased exponentially. According to AV-Test.org, new malware samples have exploded from 18 million in 2011 to 143 million in 2014. The latest research reveals that 50% of respondents believe the severity of malware infections also significantly increased in 2014.

Advanced attacks have increased dramatically - while web-borne malware attacks are still considered the most frequent, **65% of respondents say they are experiencing more APTs/targeted attacks**, an increase from the four-year average of 50% of respondents. Other significant increases include zero day attacks (an increase from 32% to 46%) and spear phishing (an increase from 48% to 55%).

Employees are the greatest source of endpoint risk

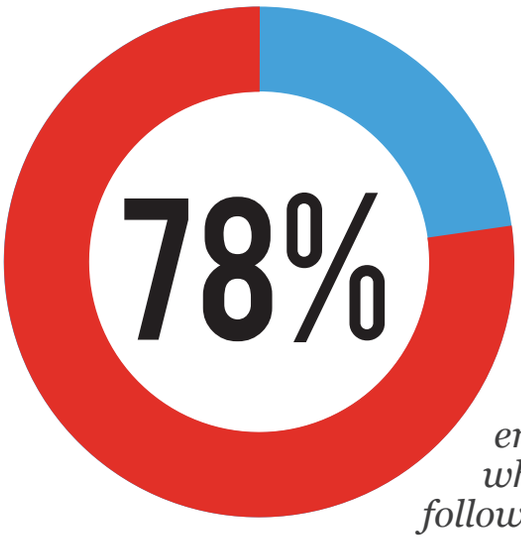
Whilst attackers are the source of threats, employees are the unwitting weak link that allows attacks to succeed. In particular, users who are careless or negligent and use multiple mobile devices with commercial cloud applications, and who work out of the office at least some of the time, form the 'ideal' vulnerability. Such users are quite common and creating a 'perfect storm' of security concerns that can be exploited by cyber criminals, and pose a complex, wide ranging threat for IT teams. One of the key findings of the research identified how the primary reason for **the difficulty in managing endpoint risk is negligent or careless employees** who do not comply with security policies and guidelines (78% agreed with this statement). They can be wilfully negligent, or simply unaware of policies, but the effect is essentially the same. This is followed by an increase in the number of personal devices connected to a network or BYOD policies, including smartphones, laptops and tablets, and often employees connect several devices to a network creating a multiplier effect. Each device is an endpoint and so presents its own security threat. They are unlikely to contain the same level of protection as company owned devices, and are less likely to be patched regularly. While bringing benefits, BYOD forms a significant part of user-centric risk. The next biggest threat was seen as employees' use of commercial cloud applications in the workplace (66%). These could have been downloaded on personal or company devices. The application environment is vast, complex and easy to exploit. In order to counter such threats, the appropriate security policies, processes and technologies need to be put in place, based on the organisation's appetite for risk.



The rise of the mobile threat

Mobile devices, such as smartphones, have seen the greatest rise in potential security risk in the IT environment. Three quarters of respondents believed that mobile endpoints have been the target of malware over the previous 12 months (up from 68% in 2013). The on-going growth of mobile is inexorably linked to an increase in security threats. IT departments find it very difficult to keep up with the growth of mobile, relying on policies which are ignored or circumvented. 68% of respondents say their IT department cannot keep up with employee demand for greater support and better mobile device connectivity, with **70% admitting their endpoint security policies are difficult to enforce**.

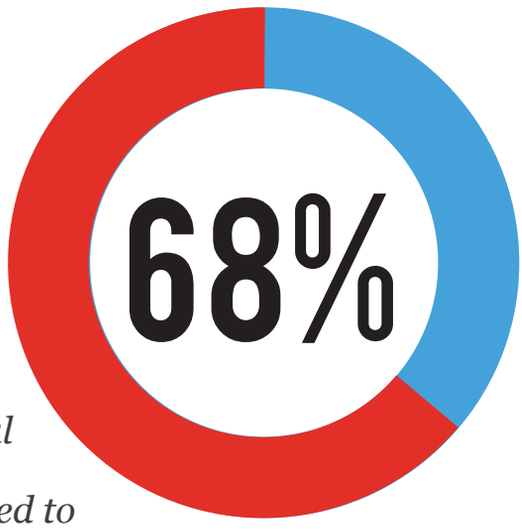
However, it may be the case that BYOD will reach a peak and flatten out. Last year, 79% of respondents believed there would be an increase in employee-owned devices in the workplace - now it's 59%. Only 21% of respondents believe company assigned mobile devices will increase. Nevertheless, for many organisations, current levels of security protection are insufficient to deal with the problems posed by employee owned devices.



The biggest threat? Our research found that...

say employees who do not follow security policies

say personal devices connected to the network



Exploitation of applications and the cloud by cyber criminals

In addition, mobile application use is also very likely to continue growing. Overall, 71% of respondents felt that most employees will continue to increase their use of commercial cloud applications. It's also very clear that the vast and increasing array of applications used by enterprise-level businesses can enable some of the most potent security threats. Last year the National Vulnerability Database catalogued 7,937 reported software vulnerabilities, a record high. Almost 94% of these were found in third party (non-Microsoft) platforms and applications.

Business and personal applications have all been targeted and pose unique threats. However, certain applications have been causing the most problems in managing endpoint risk, with 62% of respondents naming Adobe (e.g. Acrobat, Flash Player, Reader), 54% highlighting Oracle Java JRE and third-party cloud-based productivity apps (e.g. WinZip, VLC, VMware and VNC) also being listed.

Ultimately, as we transition towards an app economy, every application will become a target for hackers. Recently security researchers warned about a widespread vulnerability in Android devices that could see attackers sneakily modify or entirely replace seemingly benign apps with malware, without users becoming aware. This means a user might attempt to install a legitimate version of "Angry Birds" but instead ended up with a version that's harbouring malware. An alarming 49.5 per cent of the Android devices currently in use are at risk, which highlights why alarm bells should be ringing among corporations that have BYOD policies allowing staff to access corporate data on Android devices.

How can organisations respond to the new threat environment?

Businesses often think of security only in terms of their core hardware: servers, laptops, PCs. However, BYOD and mobile has transformed this risk, and it will be further exacerbated by uncertainty around the Internet of Things (IoT). Any device connected to the internet is an endpoint and endpoints are targets for cybercrime.

In recognition of the growing risk, endpoint security is becoming a priority – 68% of respondents said that it is becoming a more important part of their IT security strategy. Importantly, a third have acknowledged concern that their approach does not take into account the IoT.

Of vital importance is that governance and the implementation of control processes are the biggest challenges in stopping attacks on endpoints. On average, 28% of attacks on an organisation's endpoints cannot be realistically stopped with enabling technologies, processes and in-house expertise. 70% of respondents agree that their organisations' endpoint security policies are difficult to enforce - and only 11% of security budgets are allocated to malicious or negligent insiders despite the threat from employee negligence.

Future trends

In order to protect against the vulnerabilities presented by third party applications, organisations should invest in practical patch management software. While the Microsoft System Centre streamlines the patching workflow for Microsoft applications and operating system, it can often be a time consuming and complex process to build and deploy third party application patches. Other plug-ins and extensions often promise greater simplicity and effectiveness, but increase operational burdens. Instead, organisations should look for solutions that automate and streamline the patching process so vulnerabilities are plugged without requiring additional management overhead.

However, the research also revealed that organisations are evolving towards a more "detect and respond" orientation from one that is solely focused on prevention. Increasingly, the endpoint will become a security sensor that collects state or context data and uses the information to determine if it has been or is being compromised.

In addition, threat intelligence is showing signs of becoming increasingly important. In total, 64% of respondents say they have added or plan to add a threat intelligence component to their companies' security stack. Furthermore, 70% of respondents, claim that their organisations are using or planning to use "big data" to enhance endpoint and database security within the next two years.

Fundamentally, the report has shown that organisations have shifted their thinking. In addition to particular device vulnerabilities, endpoint risk is also being attributed to human behaviour. This is an important cultural shift as it shows how IT is starting to look at cyber security holistically. While it is clearly positive news that companies are making the security of endpoints a higher priority, to win the war they need to recognise the need to minimise employee negligence and invest in technologies that improve the ability to proactively detect and stop malicious attacks. An effective combined strategy must also take into account refining company policies and control processes, user awareness and overall employee education, alongside deploying new technology.

THE UNDERGROUND WORLD OF WIRELESS CONNECTIVITY

Connectivity is key. For any retail, leisure or consumer business today, Wi-Fi has moved on from an innovation, through added value and into a necessity - it's become expected. The requirement of Guest Wi-Fi now has gone further, beyond obligation and an overhead to an opportunity to engage, understand and analyse customer data on a scale never previously possible.

Replacing researchers with clipboards and expensive static advertising, Wi-Fi is the next generation in marketing to the customer standing in front of you.

Bringing 21st Century technology to the world's busiest transport system

In 2012 Virgin Media won the rights to bring the London Underground into the 21st century and launch a Wi-Fi service in the deep tunnel stations. Delivered in time for the London 2012 Olympics; it allows London Underground travellers the ability to be connected to the world above ground for the first time in 150 years.

The challenge was huge. With 4 million journeys a day, trains packed with up to 700 passengers arriving at hundreds of busy platforms at every two minutes, and devices needing to associate and users authenticate. This wasn't supplying Wi-Fi to your average business. The Global Reach Software sits at the heart of the solution, providing an award-winning customer experience that only requires customers to sign in once but still provides Virgin Media and the London Underground the ability to continue to engage with their users. Global Reach's fully resilient AAA software scales to cope with the huge demands of over 2 million travellers a day ensuring no user gets a 'Wi-Fi busy tone'. The solution provides complete mobility for users between ticket hall and platform, through all the walkways and on escalators with high availability despite the continuous associating, disassociating and re-associating as they move around the Underground, authenticating them and authorising access with tens of thousands of concurrent connections during the peak rush hour.

The platform also allows for unique, tailored customer interaction. Each mobile operator has its own registration experience all starting from the Virgin Media London Underground Captive portal, allowing curated content as well as TfL providing service updates and travel applications.

Big Data and Big Analytics

The Global Reach platform allows TfL to have full visibility of customer disclosed data such as age, gender, time of day, and usage, which helps to increase the value of the customer engagement by understanding the relationship better. This customer data is available in real-time, which means habits can be learnt and so that TfL can personalise the experience.

With over 2 million users per day across 3 million London Underground customers spanning 150 stations, the depth and richness of the data is unparalleled - and it's all available in real time. Advanced location analytics can monitor footfall in zones and target audiences with relevant promotions and offers based on where they are, how long they've been there, their age, gender and other information. Armed with greater knowledge of customer behaviours, TfL now have the opportunity to target underground commuters with relevant email marketing campaigns, all with aim to enrich the customer's journey.

The data security challenge

For any provider offering Guest Wi-Fi, there are significant security considerations. There is legislation - including the Data Protection Act, the Data Retention Regulations and even the Digital Economy Act on illegal online activity. However, it extends even further - with social media integration and the ubiquity of personal data being stored in (and transferred up to) the cloud, the importance of protecting data on Guest Wi-Fi is paramount. Choosing the right approach is not just about a simple SSID and a password written on a whiteboard, but providing greater protection for your customers' data and information more than they would do themselves.

GETTING TO GRIPS WITH TARGETED ATTACKS

Over the next few years, targeted attacks will become as prevalent as regular cyber crime threats. Cheap and easy-to-use toolkits will continue to proliferate all over the dark web, while firms of all sizes fall victim to this insidious, laser-focused scourge.

Focusing boardroom minds

In Europe, as consumers we're not as desensitised to such breaches as our transatlantic cousins appear to be. This is bad news for CIOs. It means that in the event of a breach, we're even more likely to take our custom elsewhere, or read the headlines and make a mental note never to use your services or shop in your stores.

These indirect costs can be more damaging to the breached company than the initial fines and clean-up costs. As for those, well the coming EU General Data Protection Regulation – which is mooting penalties of up to €100 million or 5% of global annual turnover – should also focus C-level minds on the security of your systems.

Why are we talking specifically about targeted attacks? Because they're incredibly difficult to spot, bypass most traditional security defences and can happen today to pretty much any organisation. Those cyber criminals who once wrote mainstream malware are now turning their hand to developing targeted attack toolkits. The reason is simple economics. Desktop operating systems are pretty well protected from mainstream viruses these days. Users, meanwhile, are increasingly spending their time on their smartphones and tablets – with the majority of data typically stored in the cloud, not on the device.

In short, cyber criminals can make a much better ROI by launching targeted attacks against companies or verticals.

Raimund Genes, CTO Trend Micro

They don't even have to be particularly sophisticated attacks. When they first surfaced, Advanced Persistent Threats (APTs) were mainly the preserve of nation states. We're talking seriously advanced technology, like Stuxnet, for example. Most targeted attacks today don't even use zero day threats – they just exploit software vulnerabilities they've found out you have.

What attack vectors are of most concern?

Firstly, watering hold attacks are flourishing - compromising a corporate web portal, embedding malware that targets employees and customers who use it for essential information exchange.
The second is island hopping, again focusing on trusted relationships by targeting a network and crossing into suppliers and customers' networks.

Attackers focus on the weakest link of the supply chain. The more reconnaissance attackers conduct on corporate supply chains, the more island-hopping attacks we will see.

Back to school

While many organisations are aware of the issue of targeted attacks, they still assume that they can get by with existing security systems: firewall, IDS/IPS, anti-malware etc. That stuff is still important for keeping out mainstream malware and attacks – in effect, cutting out the 'noise' your infosec team has to deal with. But it won't stop that targeted attack which ends up with a key customer database or a piece of critical IP falling into the hands of the bad guys.

So what is needed? Vulnerability shielding is a good start. It'll keep systems safe in case patches can't be applied quickly enough. The vulnerabilities which these patches are designed to shore up are very often the same flaws exploited in a targeted attack. It's also important to have some kind of breach detection system. You need something that features sandboxing to spot and block spear-phishing emails – which typically form the first stage of an attack – and which will scan ports and protocols to spot if an attack has already penetrated your network.

If you need any incentive, these are the tools which an insurer is likely to ask if you had following a breach.

Another approach which will gain more traction this year is that of whitelisting for the most critical systems. Work out what you want running on them and then disallow anything else that isn't on this list. It's time consuming having to manually approve each new program individually, but worth it for the peace of mind and it'll make it easier to spot when something's not quite right.


e92plus, Argent Court, Hook Rise South, Surbiton, Surrey KT6 7NL
+44 (0)20 8274 7000 | sales@e92plus.com | www.e92plus.com
@e92plus /company/e92plus
SEEN SOMETHING INTERESTING? LET'S TALK
e92plus
websense
TREND MICRO
Bitdefender
AirTight NETWORKS
XIRRUS WI-FI NETWORKS
Lumension A HEAT Software Company
global reach
UCOPIA COMMUNICATIONS
HEATsoftware