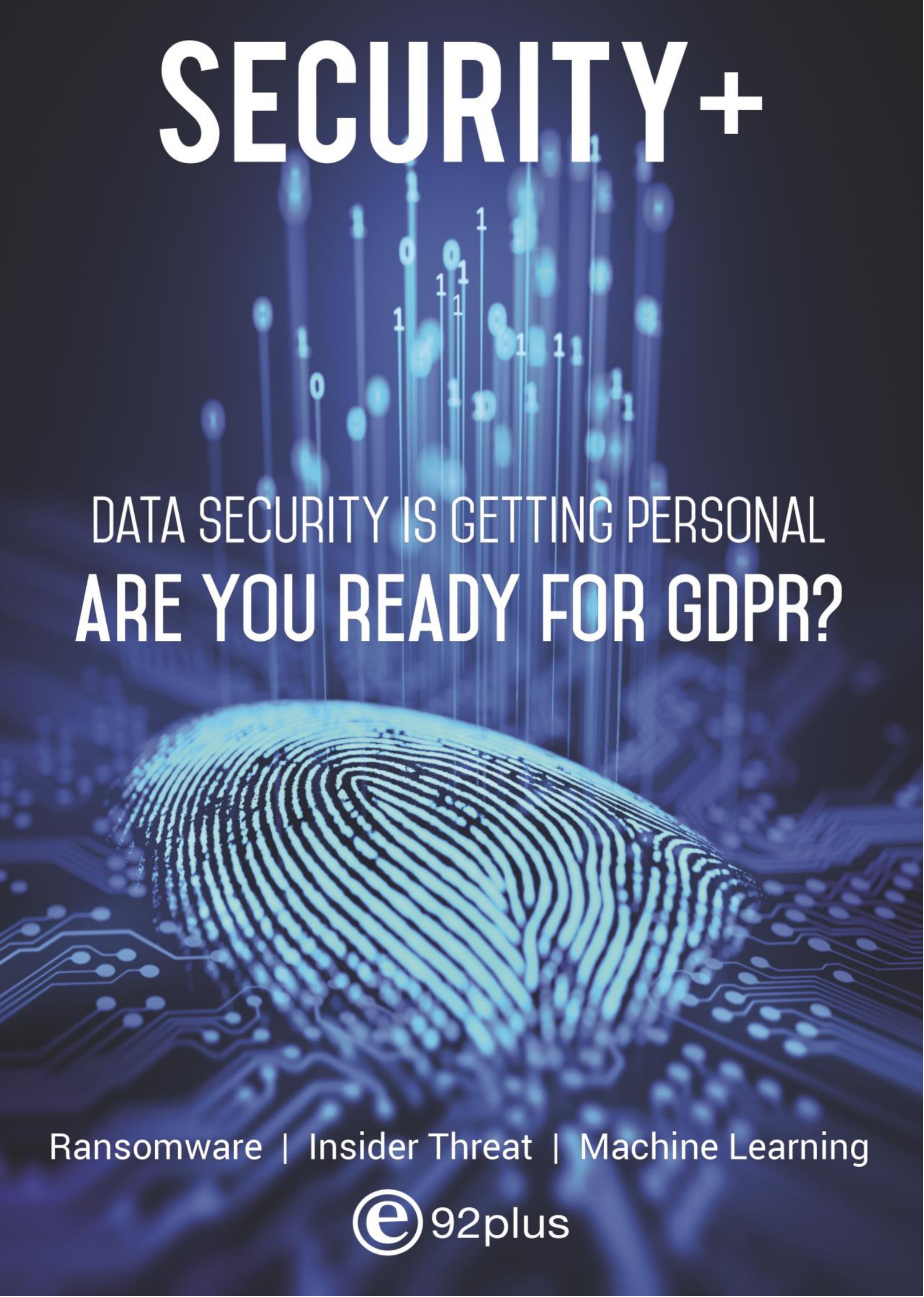
SECURITY+



DATA SECURITY IS GETTING PERSONAL

ARE YOU READY FOR GDPR?

Ransomware | Insider Threat | Machine Learning

92plus

Welcome to

SECURITY+ MAGAZINE

CLAIM YOUR FREE PERSONAL SECURITY LICENCE!

To help keep all of our readers secure, and their family protected, we are offering everyone a free personal home security licence to cover their desktop, laptop and mobile devices.

This exclusive offer, in partnership with Bitdefender and Trend Micro, is available to claim today at
www.securityplusonline.co.uk/free

Bitdefender

TREND MICRO

Welcome to the latest edition of Security+ magazine.

This issue focuses on the latest threats and challenges facing cybersecurity and networking teams - and the landscape is only getting more complex. The inexorable rise of ransomware continues, with high profile attacks (and targets) featuring in the national news, and the increasing targeting of vulnerable organisations.

Less dramatically, but arguably more fundamental, is GDPR. The new legislation is already in process, and the countdown to May 2018 is well underway. We explore the key components of the legislation, provide practical tips and explore the impact it will have on how we all provide data security.

Of course we also look at the other major trends in the industry - including machine learning, and it's potential to transform cybersecurity from defence to attack, defending wireless networks, the risks of social media and even the personal impact of the fight against cyber attacks - after all, the biggest threat is the individual, but we're also the first line of defence!

However, it's not all doom and gloom. We also explore how organisations can put in place the right defences, solutions and most importantly business processes to help defend their data, network and users. GDPR represents a significant business challenge, but also a great opportunity to put security at the heart of the organisation and help transform how we manage data security.

As usual, we'd love to hear your feedback, so please provide any thoughts, comments or suggestions to marketing@e92plus.com.

Enjoy the magazine.

INSIDE THIS EDITION

THE UK IS UNDER CYBER ATTACK, BUT THE FIGHTBACK STARTS NOW

We all know the UK is under attack on an unprecedented scale. A government report (www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year) from 2016 claimed two-thirds of large businesses had been hit over the past 12 months. The launch of the National Cyber Security Centre will help, of course. But for IT and business leaders looking to craft an effective cyber response, it's vital to know what's actually happening on the ground.

That's why Trend Micro recently interviewed hundreds of decision makers on the IT coal face. With their feedback, we produced a report which will help to reveal the scale of the problem facing firms, their key cybersecurity challenges, major areas of weakness, and what IT teams are doing to respond.

We found that the vast majority favour a coordinated, multi-layered approach featuring advanced security tools from a single, established vendor.

A cyber barrage

It's clear from those we spoke to that today it's not a case of 'if' you're successfully attacked but 'when'. Nearly half of respondents (48%) said they'd suffered a major attack over the past 12 months and over a quarter had experienced more than three attacks. Why is lightning striking several times in the same spot? Because it can. It's clear organisations are struggling to mount an effective defence of key data and systems and the black hats are only too ready to take advantage.

Unsurprisingly, ransomware and phishing were the most common attack types. But going forward things are changing. Just 8% flagged ransomware as a potential concern for 2017, suggesting messages around security best practices are getting through. But fears over targeted attacks, phishing and cyber espionage persist. These challenges are inextricably linked. And even with improved staff training, attacks can be difficult for employees to spot. So, it becomes even more important to find

"Over 25% of IT leaders had suffered more than 3 attacks in the last 12 months"

"IT leaders are most concerned about targeted attacks in 2017"

tools which not only stop malware at the door, but can also spot threats that have made it onto the network as soon as possible, to minimise their impact.

The right blend of technology and policy will also help IT leaders combat what they revealed to be their biggest challenges: a lack of understanding about cyber threats; the unpredictability of hackers; and the fast-moving nature of the threat landscape.

Layer upon layer

In a modern organisation every endpoint represents a potential gateway for hackers. It's a fact acknowledged by respondents, with two of the top three threat sources being unsecured public Wi-Fi (14%), and inadequate device security (12%). These endpoints will continue to grow as the IoT gains an ever stronger foothold in organisations. Gartner claims 3.1 billion connected things will be in place in businesses globally by the end of the year.

So what's to be done? IT leaders we spoke to claimed the mobile threat could be mitigated via things like improved staff education, enforcement of compulsory security on devices, and only allowing staff to choose from a list of pre-approved devices. Undoubtedly these will help, and IT bosses would do well to combine rather than cherry pick such approaches.

But perhaps the biggest takeaway from the report is the overwhelming support for advanced security tools as part of a layered approach. 64% of IT leaders said advanced security is effective at preventing cyber attacks, and many are already using or planning to incorporate tools like behavioural analytics and machine learning in the future.

UK firms may be faced with a seemingly endless barrage of threats from cyber space, but help is at hand.

Bharat Mistry, Cyber Security Consultant, Trend Micro . Drawing upon his experience in all areas of security, Bharat works with CISOs providing industry subject matter expertise in the development of Information Security strategies linking in depth security defences to the business requirements.

You can download the complete report free of charge from www.trendmicro.co.uk/advancedsecurity

TREND MICRO™

DANGERS FROM WITHIN:
HOW CAN BUSINESSES PROTECT THEMSELVES FROM INSIDER THREATS?

The increasing complexity and sheer volume of data breaches remain a difficult challenge for organisations across all business sectors. To combat this constant threat, companies are investing a lot of time and money on beefing up their security measures for external threats to make sure they are fit for purpose. But what about the threats which come from within?

Insider threats are a growing issue for companies, to the extent that cyber- attacks now, more often than not, are caused actively or unknowingly by employees within an organisation.

Insider threats can be among the biggest risk factors for data theft

Employees represent the biggest threat to most organisations' security, in part because insider abuse can be difficult to detect. Indeed, a recent survey of firms by Forrester found that breaches most commonly occurred because of an internal incident within an organisation – with 50 percent of breaches due to unintentional misuse or user error, known as the Accidental Insider. Examples of the Accidental Insider can be ostensibly innocent actions, such as an employee clicking on a suspicious link in an email, unknowingly downloading malicious malware or code, or employees ignoring security policy to complete work more easily.

It is not only the actions of an Accidental Insider which pose a threat. Calculating attackers can gain access to networks by targeting and manipulating employees within an organisation (or via business partners and third-party suppliers), by pretending to be legitimate when their actions are designed to steal valuable information.

Insider threats can also be a disgruntled former employee who steals data and destroys company networks by injecting malware or a logic bomb in corporate computers. Additionally, tech savvy insiders possessing in-depth knowledge and insight of an organisation's security shortcomings can sell this confidential information to external parties or black market bidders.

The increasing usage of personal devices to conduct business enhances the already complex nature of the insider threat. It creates more avenues for insiders to access sensitive corporate data, without rousing the suspicions of security teams who are often blind to that avenue.

Educate and protect employees

Although insider threats are a serious challenge to IT security, they are not just an IT issue. A significant characteristic of insider threats is that they manifest because of the human element. With this in mind, businesses must assemble an effective insider threat programme that incorporates technology controls with risk management plans and focuses on educating employees.

A successful insider threat programme will incorporate these five key elements:

- **Limiting access:** Reduce the risk of unidentified persons accessing sensitive data by limiting access to data and systems according to assigned roles

- **Policies:** Inform and educate staff on how technology, such as mobile devices and file sharing systems, should be utilised within the organisation
- **Processes:** Assign specific roles to employees to be responsible for computer/ device usage
- **Risk management:** Identify and develop a risk-management plan around mission-critical data
- **Auditing and monitoring:** When implementing the above elements, it is important to continue assessing what is effective to meet the security needs of the organisation

Collect and analyse risky user behaviour

In addition to implementing the above, organisations can also use technology to monitor and combat potential insider intrusions. Deploying database activity monitoring solutions will keep track of any suspicious changes or actions taken by employees that could signal a potential security breach. Additionally, technologies can monitor network traffic and alert IT managers of any suspicious activity or detect potential internal threats such as a sudden increase in connections to file sharing websites.

Companies can also invest in data loss prevention software which will help with the implementation of data handling policies and ensure that employees are handling data securely at the endpoint. Moreover, such software can automate the process of managing data loss policies by monitoring outbound email and blocking messages that contain sensitive information.

The seriousness of insider threats is now an unavoidable reality, so it is crucial that organisations develop a robust insider threat programme. The need to address the risks and challenges of internal dangers and effectively detect, deter and mitigate risks, both existing and new, has never been more vital.

3 MUST-DO RESOLUTIONS TO ELIMINATE INSIDER THREATS

There's no doubt that cybersecurity needs to be the heart of everyone's IT strategy - and any resolution to data security needs to encompass the ever-growing presence of insider threats. Nearly 75% of organisations are vulnerable to these threats, according to survey research from Palerra, but only 42% have the right controls in place.

I've found that organisations typically fail to establish these controls because they're daunted by the enormity of the issue, i.e., a "Where do we start?" syndrome. So I advise them to tackle it like by adopting the following three attainable and impactful steps:

Build your program's foundation upon risk management. I'm asked to attend many client meetings about insider threats, and the conference rooms are inevitably filled with IT engineers. They want to proceed with a completely tech-centric strategy, leaving out the business and "people" part of the equation. What's needed is the involvement of risk management leaders, so we can align everything we're doing to the business at hand. Through optimal risk management analysis, we determine what is unique about our organisation, and how insider threats can keep us from the pursuit of strategic goals. As part of this, you conduct an inventory to identify your data-based "crown jewels" – what are they, and where do they exist? – and develop a risk management plan to protect each one. The plan should cover not only technical solutions, but the human element.

Put someone in charge. Every ship needs a captain, right? Your initiative will go nowhere if you fail to appoint a person with proper credentialing as its manager. Again he or she may not have a deep background in cybersecurity solutions. But the manager must be capable of combining the risk management approach with a technical one to assemble a valuable and lasting insider threat response – one that remains consistent as it's applied to a cross-section of departments enterprise-wide.

Train, train, train. As promised, this is where the "people" part comes into play. You have incorporated a risk management approach. You have designated a person in charge. Now, you have to bring your program and message to those who represent the "make or break" factor in terms of future success – your employees. Because our final resolution proves so essential, let's break it down into four critical training components:

Define the insider threat. Insider threats come in many forms. They are malicious employees who intentionally steal data, sabotage systems, etc. because they were passed up for promotions and raises – or simply hate their bosses and/or jobs. There are "accidental" insiders who bear no ill-will toward their organisations, but invite compromises due to their risky behaviours. Then there are third-parties – contractors and partners whose level of risk becomes our level of risk due to our business associations and interdependencies upon systems, apps, communications tools, etc.

Illustrate what insider threat activity looks like. Here is where you educate staff about what to look for and what to do. In addressing accidental insider scenarios, include the dangers of shared passwords, the need to change them routinely and avoiding the use of predictable ones. Employees should learn about phishing scam techniques as well – where did that link come from, and how do I know if I can trust the source? As for malicious insiders, staff should know how to recognise them…is a colleague always grumbling about work or the company? Do they transfer files to a thumb drive? Are the files unrelated to his work? Do they log-in from odd locations, at odd hours?

Explain why this matters, and don't overlook the "who cares?" question as your employees will ask it overtly or quietly among themselves. Enlighten them about the potential for insider threats to trigger productivity disruptions, corporate losses, reputational damage and strategic failure - all devastating consequences which affect everyone.

Announce what the organisation is doing. Using live presentations, printed materials and online resources, walk your people through your immediate and long-term actions. Also provide helpful information through a central resource through which staffers can find out about the latest insider threat trends and even share best practices.

With a risk management "big picture" plan, a person in charge and ongoing training, you cultivate a culture of insider threat deterrence. The culture is there on the office bulletin board, it's in the office kitchenette where employees gather to talk and share, and it's in their email inboxes, as they receive the latest in related news and recommendations.

As a deterrence culture takes hold, you reduce the potential for pushback on the technologies you'll soon introduce to monitor for insider threat activity and prevent/mitigate it. Without such a culture, employees may find the technologies intimidating. But once they understand what's at stake, they'll not only accept the changes and the program in general – they'll emerge as advocates for them, as resolutions that are worth keeping.

Carl Leonard is the Principal Security Analyst at Forcepoint.

FORCEPOINT

Just how big an impact could cybersecurity threats have on your enterprise? Bigger than you think.

In February 2017, research firm Opinium surveyed more than 2,400 enterprise IT decision-makers from across Europe and the US. Some 78% of respondents had experienced at least one ransomware attack in the 12 months preceding the survey. Perhaps even more disturbing: only 10% think ransomware will threaten their enterprises in 2017.

Further, organisations are not just underestimating the ransomware threat. They are also slow to respond to actual attacks. Research conducted by the National Cyber Security Centre in the United Kingdom (UK) found that it takes organisations an average of 205 days to discover their defences have been breached.

This apparent disconnect between perception and reality is a significant obstacle to organisations trying to maintain effective security postures. And they are already challenged by flat or decreasing budgets and a cybersecurity skills gap caused by attrition of incumbent experts and the scarcity and expense of their potential replacements.

Regulations: More Hurdles to Clear

In addition to these challenges, enterprises seeking to succeed with cybersecurity are also facing government mandates, some of which include significant penalties for non-compliance. In the EU, the General Data Protection Regulation (GDPR) is going into effect in 2018, and includes reporting requirements and stiff fines for non-compliance.

- The EU GDPR applies to any company in the world using the personal data of EU citizens.
- It requires any data breach which involves sensitive personal information to be disclosed within 72 hours.
- It allows fines of up to €100 million, or 4 percent of global turnover, for any organisation that fails to comply. Those fines may exceed the £500,000 cap set by the UK's Information Commissioner's Office (ICO).
- The GDPR applies not only to a company's core network, but also to all information stored on endpoints such as USB sticks, laptops, and mobile phones.

CYBER SECURITY TODAY: A SPRINT AND A MARATHON

Charting a Course for Now and the Long Run

The GDPR is already providing guidelines for new regulations and behaviors regarding cybersecurity. According to Marsh & McLennan, Dutch authorities adopted a "mini-GDPR" in 2015. In the 130 days after the law took effect in 2016, more than 1,500 security incidents were reported by companies doing business in the Netherlands. To navigate such a complex, challenge-laden environment successfully, the most immediately useful tool a cybersecurity practitioner could ask for might just be a map.

Fortunately, such a map exists, in the form of the Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense. There are of course other respected cybersecurity frameworks and sets of recommendations. However, none has become nearly as pervasive as the CIS Critical Controls, especially the "Top 20" and "Top 5" subsets.

Derived from practices forged from actual experiences at the U.S. National Security Agency (NSA), the CIS Controls both support and reflect many of the other leading sources of cybersecurity guidance. This is, in turn, a reflection of the effectiveness and value others have gotten out of those controls. In addition, those behind the controls strive to share with and be informed by those behind many of those other respected sources.

Tony Sager is Senior Vice President & Chief Evangelist at CIS, and spend 34 years in Information Assurance at the NSA, and was an original champion of releasing the NSA's cybersecurity guidance to the worldwide public. "*[We] work with numerous companies in the threat intelligence marketplace to map summaries of what they are tracking…directly into the CIS Controls*," he said. He cited as examples the Symantec Internet Security

Threat Report and the Verizon Data Breach Investigations Report, two of the cybersecurity industry's most widely read and respected annual works. "*In fact, we provide cross-mappings from the CIS Controls to every framework we can find*," Sager said. Examples include the International Organisation for Standardisation (ISO), ISACA's Control Objectives for Information and Related Technologies (COBIT), the Payment Card Industry Data Security Standard (PCI DSS), and the US National Institute of Standards and Technologies (NIST). CIS even produces a poster that illustrates some of the links between its Critical Controls and other frameworks.

The CIS Controls are not only widely adopted and harmonised with numerous leading cybersecurity recommendations because they've been actively promoted. They are popular because they have proven effective. Here is a summary of the "Top Five" CIS Critical Security Controls, as presented on the CIS poster.

- CSC 1: Inventory of Authorised and Unauthorised Devices
- CSC 2: inventory of Authorised and Unauthorised Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

Promulgators of other cybersecurity frameworks and recommendations similarly feature these functions at or near the tops of their lists. For example, the Australian government offers a "Top 35" list of cybersecurity recommendations. Since 2010, the Australian Signals Directorate (ASD) has said focusing on four strategies addressed by those recommendations—application whitelisting, OS and application patching, and restricting administrative privileges—can mitigate at least 85 percent of cybersecurity threats. Those four strategies align with the Top Five CIS Controls.

Similarly, the UK's National Cyber Security Centre (NCSC), an arm of the country's Government Communications Headquarters (GCHQ), has published "The 10 Steps to Cyber Security" since 2012. Those steps include network security, malware prevention, removable media controls, secure configuration, managing user privileges, monitoring, and home and mobile working. These seven steps focus on areas specifically addressed by the Top Five CIS Controls.

Clickbait, clones, and cash grabs: Sidestepping the scams on social media

Uh oh, Grandma Phyllis has done it again. She just shared an ad on Facebook for discounted Ray-Bans, but you know the only sunglasses she wears are £1clip-ons from Primark. Out of curiosity, you click the link. Suddenly the red flags appear like ants at a picnic.

The domain name is not official.

When you see a domain like www.rb-store-online-sunglsses.com, you know you're in for a treat. Official brand domains are never that messy. It's only when a fake e-shop is trying to impersonate a legitimate brand, such as www.ray-ban.com, that they need to throw in a bunch of gratuitous words, abbreviations, and hyphens.

The site itself just looks bad.

Some imposter sites do a better job than others, but most of the time, they look as though their creative team did the design work on an Etch-A-Sketch. A few dead giveaways are: random fonts all over the place, multiple exclamation points (Amazing Price!!!!), capitalisation running amuck, mismatched colour schemes, confusing layouts, and so forth.

The deal is too good to be true.

Ray-Bans may not be the most expensive sunglasses on the market, but if the standard pair is about £150, then a discount of 90% would make them just £15. That's a massive discount. It's so good, in fact, that it's probably not real, since £15 would barely cover the cost of shipping. If the deal is on the official website, then that's different (and please contact me if that ever happens!). But when the domain is a hot mess, the site looks like a hot mess, and the deal is so good you wonder how they're staying in business, you've got yourself a scam cocktail.

There is no SSL Certificate.

Luckily for Grandma Phyllis, she did not input her credit card information into this fraudulent e-store. If she had, she would have seen that the http at the beginning of the URL never switched to https when she was about to checkout. The SSL Certificate is standard and exists to keep data secure, build trust, and increase the site's ranking on Google.

Dodging the bad guys on social media

Facebook is not the only place where fake companies congregate to lure unsuspecting victims. Twitter, Instagram, Snapchat, and all the other cool places to hang out digitally are fair game for bad ads and bad links.

In a Forrester survey of 192 network security decision-makers whose firms have had an external security breach in the past 12 months, 19% of security breaches were targeted through a social media account.

Here are a few tips to keep in mind so that you're not part of that 19%:

1. Don't get click-happy.
Most malware and other scams won't work unless you click on them first. That blue, underlined link just screams, "Click me!" But if it looks suspicious in any way, it probably isn't worth clicking on.

2. Report suspicious posts and block spam accounts.
Always report questionable posts to the social media site where you see them, and if the post is on a friend's account, let them know. If an account is obviously spam (e.g., "Follow4FollowLuvBird89" on Instagram), block it.

3. Set strong passwords.
The password "password" is just asking for trouble. Strong passwords are essential for keeping your accounts safe from potential threats. A strong password will use several characters and be comprised of upper- and lowercase letters, numbers, and symbols. You can still have the password "password," but it could be spelled "P@s$W0Rd823735*!!" instead.

4. Keep your firewall and anti-virus programs up-to-date.
This is one of the easiest and most effective ways to keep malware at bay.

5. Be wary of add-ons and other social media apps.
Many social media extensions and plug-ins are written by third-party companies. This is all well and good, and we're all fans of the free market, but it also lends itself to scam artists looking to pilfer your information. Look before you leap.

6. Accept friend requests only from people you know.
This seems obvious until you get a friend request from your Uncle Henry… who already has a Facebook account.

Hackers love to clone current user accounts in order to adopt all their current followers and loop them into their spam agenda. Don't fall for it! Let Uncle Henry know he's been cloned and that he shouldn't worry because his closest friends and family know he's the real Slim Shady.

In conclusion, none of us are completely immune to the various tactics of social media criminals. Whether it's Grandma Phyllis unwittingly advertising fake Ray-Bans or Uncle Henry's clone, we must stay vigilant to all the ways in which people want to steal our information.

GDPR IS COMING: HAVE YOU ASKED THESE 9 QUESTIONS?

Enforcement of the new EU General Data Protection Regulation (GDPR) goes into effect on May 25, 2018 with the potential for significant penalties for non-compliance.

As digitisation breaks down barriers and makes it easier for businesses to operate across borders, concerns about privacy are driving new legislation across the globe that may create serious regulatory and compliance challenges.

As the first, but certainly not the last, major global data privacy regulation, the GDPR is seen as a bellwether for many international businesses thinking through how they should manage cross-border data sharing, customer privacy, and sensitive data management.

Understanding data is the core of GDPR Compliance – where it resides, how it is managed, and who has access. Almost exactly one year prior to the enforcement deadline, organisations need to ask (and answer) important questions about how they are managing data. Finding the answers to the questions below will help organisations prioritise the technology solutions and investments needed over the next year to prepare for GDPR.

Patrick Dennis is the President and Chief Executive Officer for Guidance Software, directing the company's strategy and operations worldwide.

1 What counts as sensitive data?

First off, sensitive data takes different forms within every organisation. Retail firms may be most concerned with customer financial data, while pharmaceutical companies may prioritise the protection of trade secrets and intellectual property. While there are common forms of personal identifying information (PII) and personal sensitive information (PSI) like credit card numbers, social security numbers, addresses, etc., there are also unique sets of data related to intellectual property, trade secrets, or other corporate data that may be very sensitive to an organisation.

2 Where is data located, why is it stored, and how long is it kept?

Organisations need to have a clear answer to all three questions. Where data was previously stored across multiple geographic locations, now it is in "borderless" cloud data stores. Security teams also need to analyse and differentiate between private networks, cloud repositories, and third-party applications like file shares, Office 365, etc. to completely map where sensitive data is stored in a multi-dimensional landscape. At the same time, we are dealing with an exponential increase in the volume of data being created and stored. Plus, the new regulations – like GDPR – now require organisations to define the purpose for saved data and the retention period of data stored or archived.

3 Can you draw me a map?

Mapping the data landscape can be a helpful tool for organisations looking to avoid common issues with regard to data sprawl and data retention. For example, sensitive information often leaves an organisation by accident as data stored in hidden spreadsheet rows, included in notes within employee presentations, or as part of long email thread. Companies can avoid accidents like these by scanning the enterprise for sensitive data at-rest to understand where data is located, creating an accurate map, and then removing that data from unauthorised locations.

4 Who has access to sensitive data?

Organisations need to address access rights, and then assign rights based on roles and responsibilities within relevant departments or business functions. Unauthorised access to PII is a major source of risk and organisations are often shocked by who has access to information within the company. To help mitigate this risk, employee training is critical to ensure sensitive data stays with authorised personnel. Organisations need to involve HR to educate everyone about the importance of proper data handling, how it is an asset that needs to be protected, just like physical property.

5 When is data being transferred?

Perhaps the most important question for GDPR compliance deals with the circumstances around data transfer. Organisations need to understand what happens when personal data gets transferred across national boundaries, and GDPR stipulates that organisations cannot transfer this data unless appropriate protections are in place (and there are strict definitions of data transfer). For example, if a user in the United States views – just opens and views – a file located in the EU, that is considered a data transfer.

6 How is data managed?

In 2016, the Ponemon Institute found that the global average cost of a data breach was $4 million and rising. This does not include regulatory, legal, and reputational costs. While you can never fully eliminate risk, you can manage it with a data-centric approach. Protecting data and ensuring compliance is about asking simple, but inherently challenging, questions. Having a proactive data management policy, along with the right technology solutions, will make it much easier to comply with the new regulations and reduce digital risk for any business.

7 Are the right stakeholders involved, and, if not, how do I involve them?

In 2017, senior executives must prioritise sensitive data management and compliance. Ideally, organisations will already have a CISO, CIO or CSO with responsibility for information governance/data risk management (including cybersecurity). However, responsibility is currently often spread across IT, legal, HR, etc. After establishing accountability, ongoing education is imperative. Bring senior business leaders together at regular intervals for educational sessions and risk mapping to build a shared understanding.

8 What technology solutions do we need to ensure compliance?

Testing both technology and processes is an excellent way to take senior leadership one-step further. New technology is also continually evolving, and organisations should regularly review priorities, and consider how existing and new tools support changing compliance and security needs. Critical solutions needed include:

- Data Classification tools
- Governance, Risk, and Compliance (GRC) tools
- e-Discovery
- Enterprise Information Management (EIM)
- Mobile Data Management
- Collection tools

9 Are you prepared to pay?

When considering the costs and processes associated with compliance, organisations need also remember that penalties for non-compliance with GDPR can be substantially higher than other compliance penalties – up to 4% of worldwide revenue with a €20 million cap.

The digitisation of almost everything continues to ensure that cybersecurity and digital risk management will only continue to grow in importance. Those that fail to focus efforts here will likely face more significant breaches and greater costs associated with mitigation, remediation, compliance, and reputational damage.

GUIDANCE SOFTWARE

DON'T GUESS. TEST

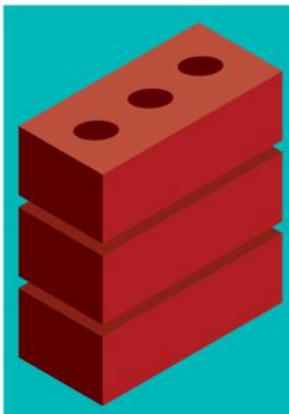
This infographic takes readers on a visual journey through their IT inventory to uncover 10 key areas that might be most prone to attack. From easily crackable passwords to vulnerable applications to risky Internet of Things technologies, businesses must ensure they are assessing their entire environment for weaknesses that could invite attacks. Instead of "guessing," organisations need to test all of these properties with powerful managed security services and technologies.

REDUCE THE RISK

Vulnerabilities in databases, networks and applications introduce security weaknesses that can increase your data breach risk.

81% of businesses failed to detect data breaches themselves in 2014.

BUILD SECURITY INTO IT PROJECTS



77% of IT pros have been pressured to unveil IT projects that were not security ready.

SECURE YOUR INTERNET OF THINGS

Whether it's smart toilets, ATMs, WiFi-connected homes or business automation systems, Trustwave has tested many internet of things devices that lacked often-times basic security controls. Consumer and business products shouldn't hit the shelves before they're tested for security vulnerabilities.

THE CLOUD NEEDS TESTING TOO

47% of IT pros were pressured to use or deploy cloud-based solutions.

CHANGE CAN INTRODUCE NEW VULNERABILITIES

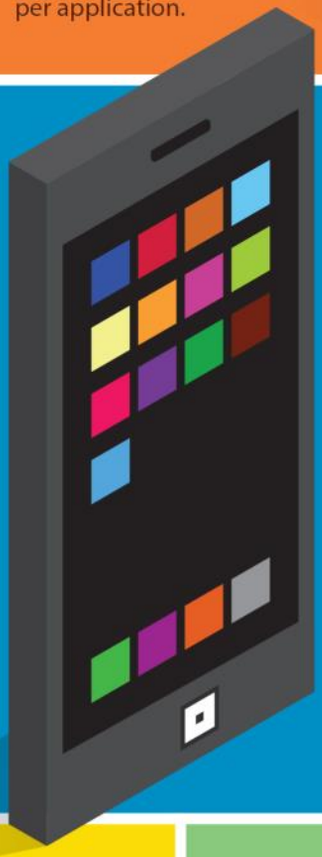
Infrastructure changes introduce new vulnerabilities. If you don't test, and test often, you're likely putting your business at risk. Constant vigilance through testing puts you ahead of attackers.

PROTECT YOUR WEB APPS

98%

of web applications tested by Trustwave were vulnerable with a median number of 20 vulnerabilities per application.

GO MOBILE, SAFELY



95%

of mobile applications tested by Trustwave were vulnerable.

PROTECT YOUR DATABASES

Cyber-criminals are after data – sensitive, valuable and saleable data. Configuration mistakes, identification and access control issues, missing patches or any toxic combination of settings can lead to escalation-of-privilege or denial-of-service attacks, data leakage or unauthorized modification of data.

70%

of IT pros believed they were safe from cyber-attacks and data compromises.

AVOID GETTING LULLED INTO A FALSE SENSE OF SECURITY

PLUG THE PASSWORD PROBLEM

"Password1" is the most common business password, and 39% of passwords tested were only eight characters long. It takes only one day to crack an eight-character password but an estimated 591 days for a ten-character password.

Trustwave

MACHINE LEARNING: THE HOLY GRAIL FOR CYBER SECURITY OR JUST HYPE?

Every now and then a technology comes along that deserves the hype it attracts – arguably machine learning is one of them. The premise is simple – cyber-attacks are increasingly sophisticated and creative, while good at concealing their true intentions. The use of automation takes the heavy lifting out of detecting anomalies, to spot them and protect against attacks. If it works, it can be used to identify everything from known to zero-day attacks. Used correctly and efficiently, machine learning levels the playing field for security teams as, at the moment, the criminals appear to have an unfair advantage. However, this also means everyone is clambering aboard the bandwagon, and sometimes marketing promises don't match technical reality.

Start with a definition

The main question is - what should constitute a definition of true machine learning and how does it differ from the hype?

To answer this, it is important to strip things back to their simplest form. In computational and statistical terms, machine learning encompasses any algorithm that gives technology the ability to learn from multiple data sets and create statistical models that the technology then uses to make accurate predictions. Practical applications range from predicting the weather, financial markets and even protein homology detection in human genome sequences. In the world of cybersecurity, where picking out microscopic irregularities from floods of data is vital, the ability to learn and take action, as opposed to requiring input from an already overburdened security team, is where the true benefit and application of machine learning lies.

However, this is also where the promise can differ from the reality. Often marketing teams will label something which can parse big datasets and come up with broad conclusions, to be acted on by a security team, as machine learning. The problem with this is that it still requires people to make decisions. The heavy lifting is only partially done. Whilst it sounds nuanced, this is an important distinction.

To that, add context

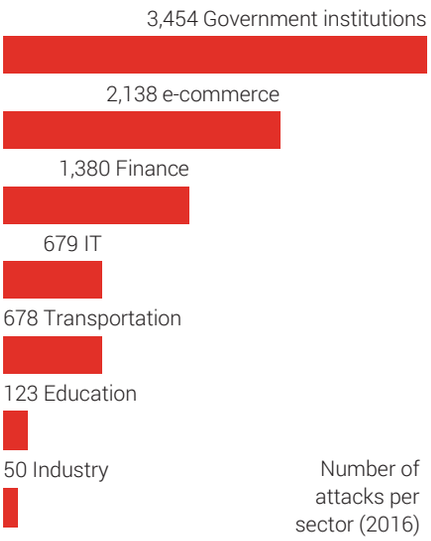
When assessing the promise of machine learning in cybersecurity, it's important to take into account the threat landscape, which has become a game of spotting a needle in a haystack. Take the example of protecting the software your organisation runs from attack. Enterprises are now rolling out more and more applications, the issue is that any erroneous line of code used on your website or internally presents a possible route of attack. This presents a huge amount of potential flaws for attackers to abuse. One poorly constructed piece of code can be the start-point for a full breach, which can wreck reputation and cause financial damage.

The attacks aimed at this code are numerous, unpredictable and have multiple 'parts' involving a mix of human creativity and technology. One day can see a single 'script kiddie' curious as to whether an idea they have is possible, another sees teams of well-resourced attackers using custom developed exploits. A lot of these attacks may never have been seen before, all use an assortment of separate elements.

Against this hectic backdrop, defence is predicated on the need to make sense of lots of seemingly unrelated actions and act with speed and autonomy. This is where true machine learning comes into its own. Only by being able to correlate seemingly random markers of an attack, put them together in context and decide whether to take action, can attacks be foreseen and stopped. Just recording large datasets and flagging actions as potentially anomalous is not fast or accurate enough. By then it's too late.

To put this in lay terms, it's akin to being able to predict the weather. A person doesn't need to be told that the wet drops falling from the sky might be rain because it looks similar to a database of rain pictures, followed by a suggestion to go inside. By then, it is too late and you are wet. True machine learning would instead look at the context – air humidity, precipitation rates, air pressure patterns, time of year, or whether people are wearing coats and running inside – and direct you inside.

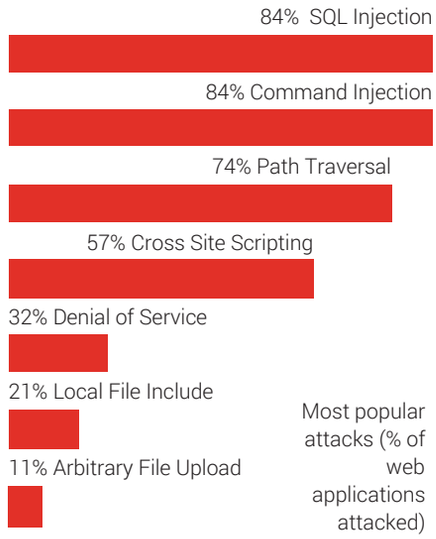
In a world of increasing cyber-attacks, getting rained on means brand damage, financial loss or even catastrophic outages. People need to look beyond the marketing and question whether they are truly getting self-learning technology with effective practical application, or just buying the promise. Machine learning can really help put organisations the world over not just back in the game, but give them a competitive edge. The only caveat is the promise must match the reality.



When you read cybersecurity news, these thoughts probably crossed your mind: how do they estimate efficiency of security tools or damage caused by hacker attacks?

Each year Positive Technologies specialists conduct hundreds of studies analysing security of networks, devices, and applications as real hackers would do.

Perhaps most worryingly, the latest report showed that all the web applications tested contained at least medium-severity vulnerabilities. 70% of the systems studied had a critical vulnerability, and the percentage of systems with this type of vulnerability has grown consistently over the last three years.



WEB APPLICATION ATTACK TRENDS

Vulnerabilities in the Internet-connected software run by large organisations create a large security risk. A single successful exploit — which can be as short as a few characters typed in the wrong place — can abuse these flaws and set a breach in motion. Exploits can be leveraged to access corporate databases and other sensitive information, causing financial and reputational damage to the target, system hijacking, theft of intellectual property, and downtime. Visitors to the websites of these companies can also be put in danger, since successful attacks can result in theft of credentials and malware infection of user computers.

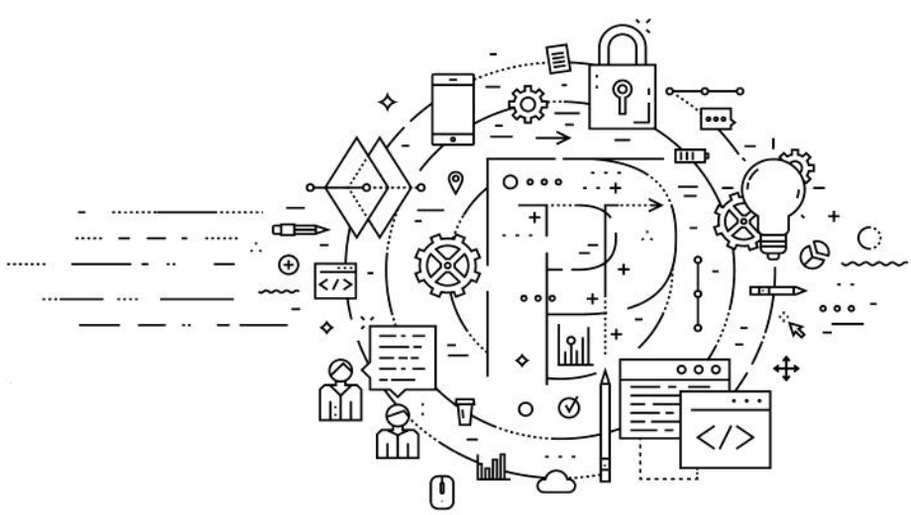
The aim of the web application attack research was two-fold: to determine which attacks are most commonly used by hackers in the wild, and to find out which industries are being targeted and how. With this data, organisations can be more aware of digital threats and protect themselves accordingly.

Summary of findings:

- Organisations across the board are being targeted with a high volume of attacks on their web applications.
- Governmental organisations and e-commerce companies showed themselves to be particular targets. These two sectors are also subjected to the highest level of manual (non-automated) compromise attempts.
- Attack types are tailored to specific sectors. For example, e-commerce sees a mix of attempts designed to cause downtime and access internal files. By contrast, 65% of all attacks in the finance sector attempt to steal the login information of website visitors.
- Sectors seeing the lowest attack volumes, conversely, see the highest volume of automated web attacks from hackers, who use specialised software to search for vulnerabilities automatically.
- Easy-to-execute methods such as SQL Injection and OS Commanding are the most commonly used methods across all sectors. Rarer attacks include Arbitrary File Execution and Cross-Site Request Forgery.

The results make clear that hackers target certain sectors more than others: specifically, those bringing the most return in terms of sensitive information or financial reward. This is not a new trend in the cybersecurity space, but unfortunately one that will continue to drive malicious activity. Attackers are beginning to show a higher level of technical competence and capabilities in their attempts to steal funds and sensitive data in web application attacks.

In order to accurately construct attack chains and perform incident forensics in such a fluid environment, including advanced persistent threats, it is important to implement technological solutions able to successfully correlate a vast range of variables and take appropriate countermeasures with minimal human intervention.



THE FUNDAMENTALS OF WI-FI TROUBLESHOOTING

"The Wi-Fi is slow" is a common complaint. Poor performance on a Wi-Fi network has many different causes, some of which include:

- APs using legacy data rates such as 1 and 2 Mpbs
- Too many devices transmitting on the same channel
- APs transmitting too high of power level
- A high retry rate of transmissions

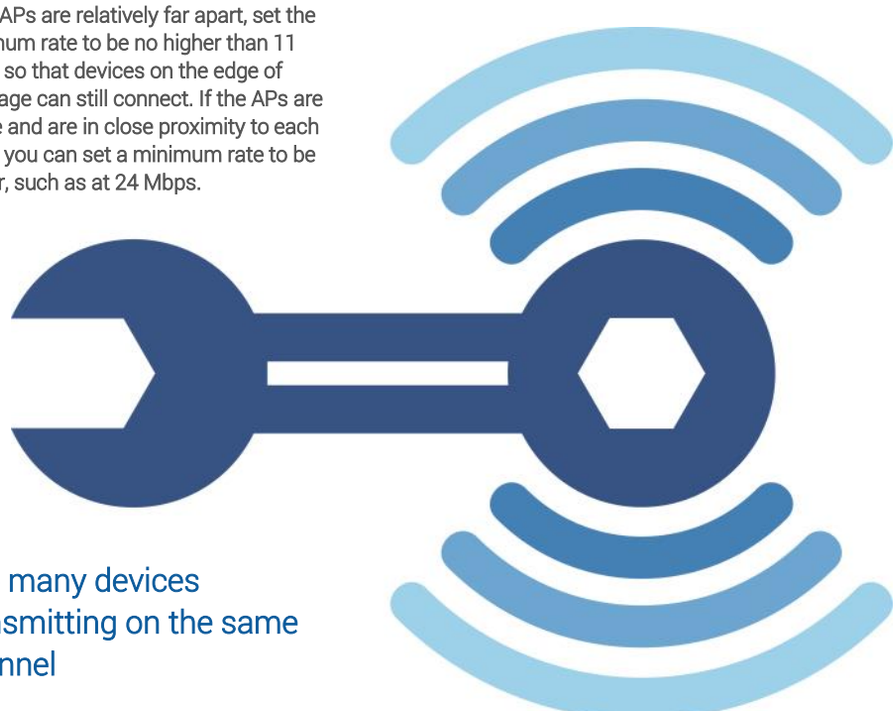
Access Points using legacy data rates such as 1 & 2 Mpbs

Newer Wi-Fi devices are continuously being designed and delivered to be faster than before. But older devices that are considered "slow" by today's standards are still out there, and many Wi-Fi networks by default still support them. This means the networks' access points (AP) support connections at slow legacy data rates such as 1 and 2 Mbps. This, in turn, can cause Wi-Fi devices that are far from the AP to connect at very low rates, and very old devices to connect at very low rates. Such connections can slow things down for everyone on the network.

When troubleshooting a slow performance issue, or when optimising a Wi-Fi network for best performance, **one of the first and simplest things you can do is check the data rates that the APs support.** When you select the network you are testing, you need to view the list of APs on that network, and check the supported rates. These rates are in Mbps and include 1, 2, 4, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. These rates include the basic rates (which a client device must support in order to connect) and extended supported rates.

To improve performance of the network for all devices, **consider disabling the lower rates on your APs.** This must be done carefully to ensure that devices that must connect are still supported. For example, some environments must support 802.11b devices which require 1 Mbps connection rates. But if really old devices are not required to be supported, you can set the lowest rates at 11 or even 24 Mbps. How low depends also on AP density.

If the APs are relatively far apart, set the minimum rate to be no higher than 11 Mbps so that devices on the edge of coverage can still connect. If the APs are dense and are in close proximity to each other, you can set a minimum rate to be higher, such as at 24 Mbps.



Too many devices transmitting on the same channel

One common cause is the fact that airtime is shared among all Wi-Fi devices on the same channel in the same area. If too many devices are trying to transmit on the same channel, performance will slow down for everyone. Having too many APs on the same channel in the same area is known as co-channel interference (CCI), and you want to reduce this to optimise performance. However, in the 2.4 GHz Wi-Fi band, there is another problem source known as adjacent channel interference (ACI). Adjacent channels in the 2.4 GHz band overlap with each other, so that traffic on one channel can interfere with traffic on a nearby channel. A best practice in 2.4 GHz is to use only channels 1, 6, and 11 because these channels are far enough apart that they do not overlap. But if an access point is on channel 2, 3, 4, 5, 7, 8, 9 or 10, it will overlap and interfere with an AP on channel 6. This is adjacent channel interference, and can cause more performance degradation than co-channel interference. It is better to have 3 APs on channel 6 than to have one each on channels 4, 6, and 8, for example.

APs transmitting too high of power level

Your network customer/user is complaining that they cannot connect to the Wi-Fi network. You go on-site to consult with this user to understand why. At their specific location, you see that their Wi-Fi client is showing 4 bars from the network to which they are trying to connect. If you are really serious, you might even pull out a signal meter on your phone app to see the actual signal level of that network in terms of dBm. It all looks good. So why no connection? One of the network's access points (AP) may actually be transmitting at way too high of power level, resulting in the 4 bars and high dBm measurements at the user's location.

This will also cause the user's client to try to connect to that specific AP. However, does that AP hear the user's client? **Wi-Fi communication is a two-way street, and ideally both the user's client and the AP and should be transmitting at similar power levels.** Commonly, the user's client should see the strongest signal level on the network from the AP that is closest to them. If you measure the user client's signal level at the location of that AP, you should see a similar signal level. If you see a signal level that is way too low (e.g., less than -80 dBm) or none at all, there is your problem!

A high retry rate of transmissions

Good Wi-Fi connections and high performance depend on a well-designed network. This means strong coverage, minimum interference, minimum airtime contention and good network capacity. When conditions go south, Wi-Fi devices will transmit but their transmissions are not received. When a Wi-Fi device, either an access point (AP) or a client, transmits a frame of data, it must receive an acknowledgement from the receiver. If it does not, it will re-transmit that frame of data. This is known as a retry. The retry rate is the percentage of total frames transmitted that are retries. A high retry rate means that much of the precious airtime is used (or wasted) by duplicate transmissions because the conditions are not allowing a transmitted frame to be properly received and acknowledged.

While there is no set standard on a good vs bad retry rate, **if the measured retry rate of the connection is more than 15%, you should start looking at other issues like poor SNR, too many APs on a channel, too many clients on a channel, or high channel utilisation.**

For more information on Troubleshooting 802.11ac Wi-Fi, watch this recorded webinar on Brighttalk: https://www.brighttalk.com/webcast/5522/208803

BYOD: MEETING THE NETWORK CHALLENGE

Bring Your Own Device (BYOD) schemes tap into employees' desire for freedom, flexibility, and remote working. They help to blur the once-clear distinctions between home and workplace, boosting productivity and enabling people to work smarter and better by integrating work with life outside of the office. Organisations like and want BYOD and it saves them money if employees' use of their own, preferred devices negates the need to constantly purchase or upgrade corporate desktops, for example. However, IT professionals have previously seen BYOD as a threat, not a leadership opportunity.

Now that BYOD is becoming more pervasive, it certainly brings its own challenges – which is precisely why it demands strong leadership. The data security challenges alone are complex, and yet many IT professionals find themselves reacting to BYOD, rather than actively leading it from the front, where driving the business advantage and agility presents a real opportunity.

Doing nothing is not an option, because the problems caused by any failure to lead and manage BYOD pose too big a risk. For example, BYOD can be a drain on network performance and resources if devices, access policies, and usage are not properly managed and monitored. More, the growth of 'shadow IT' – employees' use of ad hoc, unsanctioned technologies – can lead to financial penalties in today's highly regulated world if sensitive data is lost, stolen, or shared insecurely with unauthorised people.

Network Stresses

Network performance can be the most obvious impact of BYOD. In established organisations, legacy networks will have been planned around known assets and standards, and not for what some might see as a technological 'Wild West' of different devices, OSs, and apps. The speed of change means that the device that an employee uses today may not be the device they use tomorrow, which means engineers hitting a moving target in terms of network performance. In that environment, taking a holistic, forward-looking view is the only realistic option. After all, IT teams and network engineers need to maintain network performance, speed, reliability, and uptime for all, and not just for those employees who want to use their own devices. A slow, jittery, or unreliable network won't just impede employees' work from day to day, it may also erode their productivity and performance of the organisation as a whole.

But there are two problems:

1. End users' network experience is not determined solely by the performance of the wireless portion of the network. The underlying wired network connecting the APs also plays a part, as do the servers hosting cloud applications and data.
2. Not only is there more competition for wireless channels and bandwidth, some devices may eat up more network resources than others, restricting or slowing access for everyone else. In this way, the IT teams' culture of 'making do today' needs to be replaced with one of planning for tomorrow by stress-testing the network for the future demands of next-gen devices. This is why intelligent performance-monitoring tools are vital. If IT professionals can monitor the network for surges – for example, in the middle of the night, which might suggest a hacking attack – then security and performance can be properly managed and maintained.

Business Challenges

There are also many other significant impacts on the network - from regulatory requirements (including GDPR and the management and security of personal data), to changes in working cultures (not least the use of "private clouds") and even policy management - do employees know what they can and can't do on the corporate network?

Conclusions

Legacy network management systems just don't cut it in the world of BYOD, and neither do the plethora of vendor-specific tools that may come with some enterprise applications. Instead, IT teams should refocus on the user, on management, and on implementing policy. The answer is end-to-end visibility across the entire physical and virtual infrastructure and a proactive approach: it's all about identifying problems proactively: being able to pinpoint where the problem is quickly solves a lot of problems in the 'war room' and reduced the finger-pointing.

For IT leaders and their teams, this level of visibility and transparency is essential, but that demands having access to dedicated tools and a fast, robust network. Rather than chase down problems once they have occurred, it should be possible to prevent them happening in the first place. In this way, BYOD can truly be an asset to the organisation, not a brake on network performance and security – and it will be one less headache for the IT professional!

NETSCOUT

CORPORATE RANSOMWARE ATTACKS ARE THE NEW NORMAL

WHAT TO EXPECT NEXT

For the past two years, ransomware attacks have grabbed the headlines of international news, showing that cyber-criminals have shifted their attention to targets that not only need their data back, but also have the financial power to pay the ransom.

To date, education is one of the most targeted industries by cyber-crime, closely followed by government, healthcare, finance, retail and energy. However, no industry is safe from this threat, with cybercriminals leveraging the fact that the balance between IT spending versus IT security tips in the attacker's favour.

To the hundreds of cases reported by the media, hundreds of others who have remained unreported are piling up as organisations seem to remain oblivious to the ransomware threat. Oddly enough, only 38% of organisations currently have a strategy to deal with destructive malware, as compared to 43% in 2015, according to recent surveys.

Are organisations easily giving in to ransomware?

According to Bitdefender, some 50% of infected consumers are willing to pay to regain access to their encrypted files after being hit by ransomware. The same is true for companies, most of which won't be able to function in the absence of data. For instance, one hospital paid a ransomware attacker more than $17,000 to recover patient files that were necessary for treatment. The amount of money might sound diminutive when put into perspective, but this is just one incident out of many where management decided to be transparent about the breach rather than fix it internally and hide it under the rug.

Although the FBI encourages victims not to give in to threats, as paying the ransom would only further incentivise cyber-criminals to ramp up their efforts, giving in to ransom is the only way an organisation can go back to normal in the absence of disaster recovery policies. Which makes matters worse.

Ransomware is becoming more and more sophisticated

New ransomware strains have not been limited to only encrypting sensitive files, such as documents, databases, or even pictures. In order for crypto-ransomware to become more competitive in an already saturated market operated by thousands of cybercrime groups, it has to go beyond encrypting individual files. This is the case with the Petya ransomware, which shows how cybercriminals have shifted focus towards restricting users from accessing information from the entire disk. Specifically, it encrypts the NTFS Master File Table to further pressure the victim into paying because it wouldn't even allow them to use the operating system, let alone to access the data.

What to expect next?

If you are an IT decision maker in an organisation, you probably have a hard time keeping your infrastructure, your customer's information and your intellectual property safe from harm. If right now ransomware is one of the most serious threats companies and individuals face, things will only get worse in the short to medium time, as this business model reaches saturation and companies learn the importance of backups.

However, Bitdefender predicts that by 2018, ransomware will evolve into extortionware – having your data stolen and likely to be exposed on the Internet unless a ransom is paid. This form of extortion would leave businesses even more vulnerable and likely to end up settling, as having intellectual property or confidential documents exposed online could be far more damaging to a company's reputation and financial stability than the cost of recovery from a traditional ransomware infection.

To this end, regardless of an organisation's size, proactively setting up new security and back-up mechanisms that can detect and rapidly mitigate such infections are more than recommended.

Bitdefender

TODAY'S THREAT PROTECTION TECHNIQUES:

THERE IS NO SILVER BULLET

The security landscape changed dramatically with the maturation of crypto-ransomware in 2014. Not only did this new type of malware bring about a more lucrative business model for attackers, it also spurred the adoption of many so-called 'next-gen' endpoint security techniques. While these techniques bring impressive new capabilities to the fight against malware, is there a 'silver bullet'?

The security landscape used to be black and white: traditional anti-virus signatures and web filtering protected against 'known bad' entities; whitelists and application control ensured users were exposed to only the 'known good' files. But as the IT environment becomes more sophisticated, so do the threats faced by businesses of all sizes - and most concerning is the way attackers are now looking at their 'work' as a business — and investing a considerable amount of money into evasion techniques that allow them to slip through the security measures put in place by most organisations.

The new business model for attackers

Security vendors have seen a fundamental shift in the commodity malware industry in recent years. One moment stands out in particular: the introduction of crypto-ransomware in 2013 (and its maturation as a viable method of attack), which dramatically changed the business model for attackers. Consider the ways a malware infection can be monetised:

- Rent out infected servers to send spam, launch distributed denial of service (DDoS) attacks or mine for Bitcoins
- Steal money directly from the victim (e.g. through a banking trojan)
- Steal the victim's data or IP
- Ransom the files on the victim's computer

Each approach has different costs, risks and potential rewards for the attacker. It takes a lot of infrastructure to control and maintain a botnet of infected servers — and the prices people are willing to pay for spambots and 'DDoS-for-hire' services are typically quite low. Meanwhile stealing money directly from a person's bank account is lucrative but requires a complex system to launder the money, while stealing IP necessitates finding data that has value -and that has a buyer willing to pay for it.

In comparison, ransoming a computer and its files allows attackers to quickly realise a premium price per infection (typically between $500 and $1,000 for decryption keys) and get paid immediately in Bitcoin, which can be anonymised using a Bitcoin scrambler to ensure the transaction can never be traced.

The evasion and detection arms race

Due to the fast return on investment of crypto-ransomware, attackers are able to re-invest their 'earnings' into new evasion techniques. Many attackers no longer rely on free or cheap botnets, instead compromising or purchasing legitimate infrastructure from which to launch their attacks: Compared to the past with links in spam emails directing to dodgy websites, attackers now compromise legitimate web servers, which then redirect their victims' browsers to the malicious website.

Social engineering attacks are also on the rise, which see people tricked into handing over their confidential information through fake web pages that replicate the look and feel of banks, government agencies or utility companies, complete with CAPTCHA fields or obfuscated JavaScript to avoid detection.

Another concern is the use of polymorphic malware 'hash factories', which can automatically change the characteristics of their malware files on a regular basis — as quickly as every 15 seconds, in the case of the Cerber crypto-ransomware. By constantly inserting new pieces of code into the malware, it becomes practically impossible for traditional, static, signature-based detection to keep pace. Other new techniques include splitting the crypto-ransomware's main malicious logic into multiple sequences and 'packed' malware that combines code with long strings of data.

By abusing legitimate web services and creating malware that can easily avoid detection, attackers have upended the traditional IT security paradigm. What is good anymore? The dividing line between black and white has been muddled — resulting in a constantly growing 'gray' area that is much harder to defend against.

Responding to the gray

In response to the proliferation of gray-area threats, security vendors have developed a number of so-called 'next-gen' threat-protection techniques in recent years: sandboxing, behaviour monitoring and vulnerability shielding, to name a few. While these have all added impressive new security capabilities to the mix, it's important for enterprises of all sizes to recognise that no one next-gen technique can possibly protect against every threat.

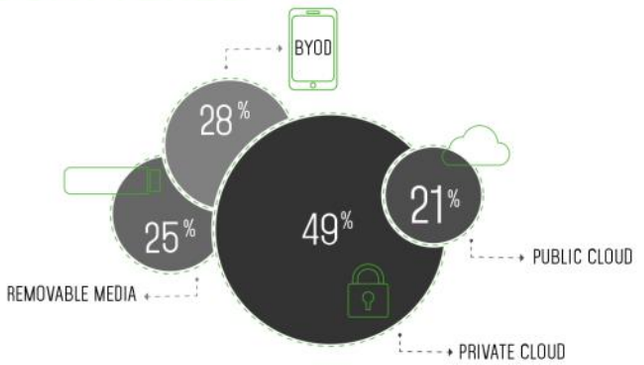
As analysts such as Gartner's Neil MacDonald have been saying for years, a multi-layered, defence-in-depth approach to security is the best way to ensure maximum protection. This means having many different security techniques working together and complementing each other to catch the highest possible percentage of malicious elements. If an organisation relies on just one or two techniques for its security needs, there's a much greater likelihood something bad will slip through the cracks — with potentially devastating consequences.

And as MacDonald points out on the Gartner blog, relying on a single vendor for endpoint security does not lead to a loss of defence-in-depth. Instead, an integrated endpoint protection platform can help organisations eliminate the gaps in security coverage and visibility that can occur when using a mix of different point products — all while achieving significant cost savings and operational simplification.

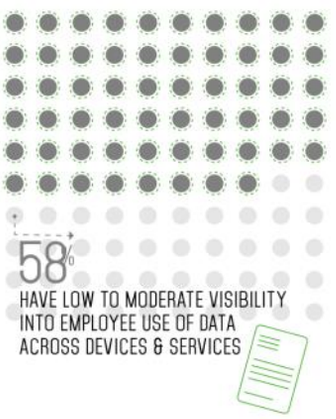
RESEARCH SHOWS UNDERSTANDING BEHAVIORS AND INTENT IS CRITICAL TO FUTURE OF CYBERSECURITY – BUT SIGNIFICANT GAPS EXIST.

OF THE 1,252 CYBERSECURITY PROFESSIONALS SURVEYED....

CRITICAL BUSINESS DATA IS SCATTERED

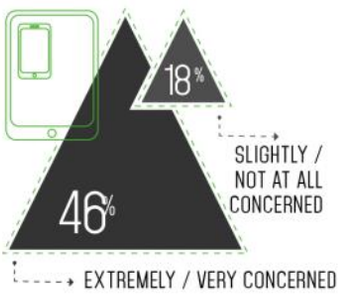


REDUCED VISIBILITY



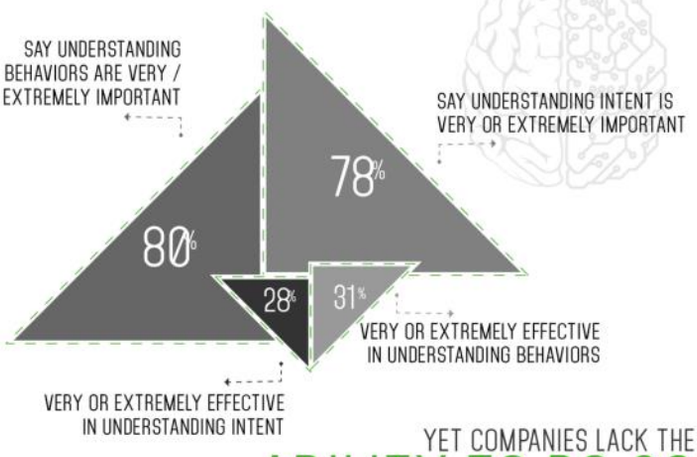
58%

HAVE LOW TO MODERATE VISIBILITY INTO EMPLOYEE USE OF DATA ACROSS DEVICES & SERVICES



PERSONAL & BUSINESS DATA CO-MINGLING ON BYOD DEVICES

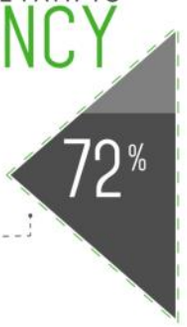
UNDERSTANDING BEHAVIOR & INTENT IS VITAL



BIG DATA CANNOT FILL SECURITY GAPS

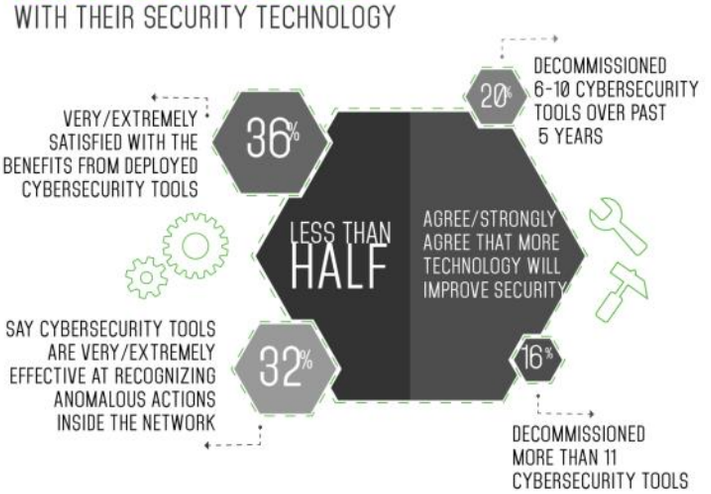
YET COMPANIES LACK THE ABILITY TO DO SO

UNDERSTANDING BEHAVIOR & INTENT: THE PATH TO SECURITY EFFICIENCY



AGREE OR STRONGLY AGREE THAT FOCUS ON BEHAVIOR & INTENT WILL IMPROVE SECURITY & REDUCE COSTS

COMPANIES ARE NOT SATISFIED WITH THEIR SECURITY TECHNOLOGY



LEARN MORE AT WWW.THEHUMANPOINT.COM

FORCEPOINT
POWERED BY Raytheon

GETTING PERSONAL IN THE CYBERSECURITY BATTLE

INSIGHTS FROM THE 2017 SECURITY PRESSURES REPORT

The saying goes that time flies when you are having fun, yet it feels somewhat peculiar and ungainly assigning a lighthearted term to describe the daunting work of IT and security professionals like yourself.

Trustwave commissioned a third-party research firm to survey 1,600 full-time information technology (IT) professionals who are security decision makers or security influencers within their organisations. Each year since this annual report was first published, a majority of respondents have reported that the amount of pressure they experienced in regard to their security increased from the prior 12 months. More often than not, IT and security professionals are feeling the heat when it comes to protecting their organisation against a wide range of adversaries and threats.

The new study shows that while 53% of respondents report increased pressure in trying to secure their organisation, there has been a shift in the source of this stress. Security is now becoming more personal, with 24% of respondents citing pressure exerted by oneself as the second-biggest human pressure pusher, up 13% from the previous year. This is compared to 46% citing the most people pressure coming from boards, owners and C-level executives, which dropped 13% in the last year. This shift in pressure highlights that individuals may be starting to understand the bigger role they play in helping to enable their organisation's security posture.

27%

LACK PROPER IN-HOUSE RESOURCES

42%

FEAR REPUTATIONAL DAMAGE FOLLOWING A CYBERATTACK

Key findings from the 2017 Security Pressures Report from Trustwave include:

Daunting repercussions for individuals and businesses alike: 42% of respondents cited their biggest fear following a cyberattack or breach was reputational damage to themselves and their company. This fear took the lead ahead of financial damage to one's company (38%) and termination (11%).

Managing on a global scale: 31% of respondents partnered with a managed security services provider (MSSP) to help compensate for lack of skilled security professionals, while 26% of respondents are involved in a partnership between in-house teams and an MSSP.

Quality over quantity: Shortage of security expertise has emerged as the second biggest pressure facing security pros at 15%, behind advanced security threats at 29%. Although companies are facing a large skills gap, 24% of respondents would rather increase the security skills among staff members rather than increase their staff (3%), confirming the desire to grow their skills versus throwing bodies at the pressures they face.

Progress in prioritising security over speed: 65% of respondents felt pressure to roll out IT projects before they had undergone necessary security checks/repairs, compared to 77% over the previous two years. 35% of respondents did not feel pressured to deploy new technology quickly, up 12% from last year.

Latest and greatest: Pressure to select security technologies containing the latest features dropped from 74% in last year's report to 64% this year, despite 27% of respondents citing that they lack the proper in-house resources to effectively use them

Computer kidnapping: 30% of respondents rank customer data theft as the most worrisome outcome of a cyberattack or data breach. Next is ransomware, for which 18% of respondents view as the most unsettling post-incident consequence.

31%

PARTNERED WITH A MANAGED SECURITY SERVICES PROVIDER TO HELP COMPENSATE FOR LACK OF SKILLED SECURITY

"*Findings show that the pressures cybersecurity professionals face have become much more personal than in previous years, as executives recognize that pressure does not translate into better performance – instead it may lead to stress, burnout, and faults*," said Chris Schueler, senior vice president of Managed Security Services at Trustwave. "*My advice to those facing these pressures head on is to no longer think of security as a siloed discipline. Partnering with a managed security service provider can help compensate for and amplify areas of your security program that you find too complex or lack the internal resources to address.*"

Trustwave