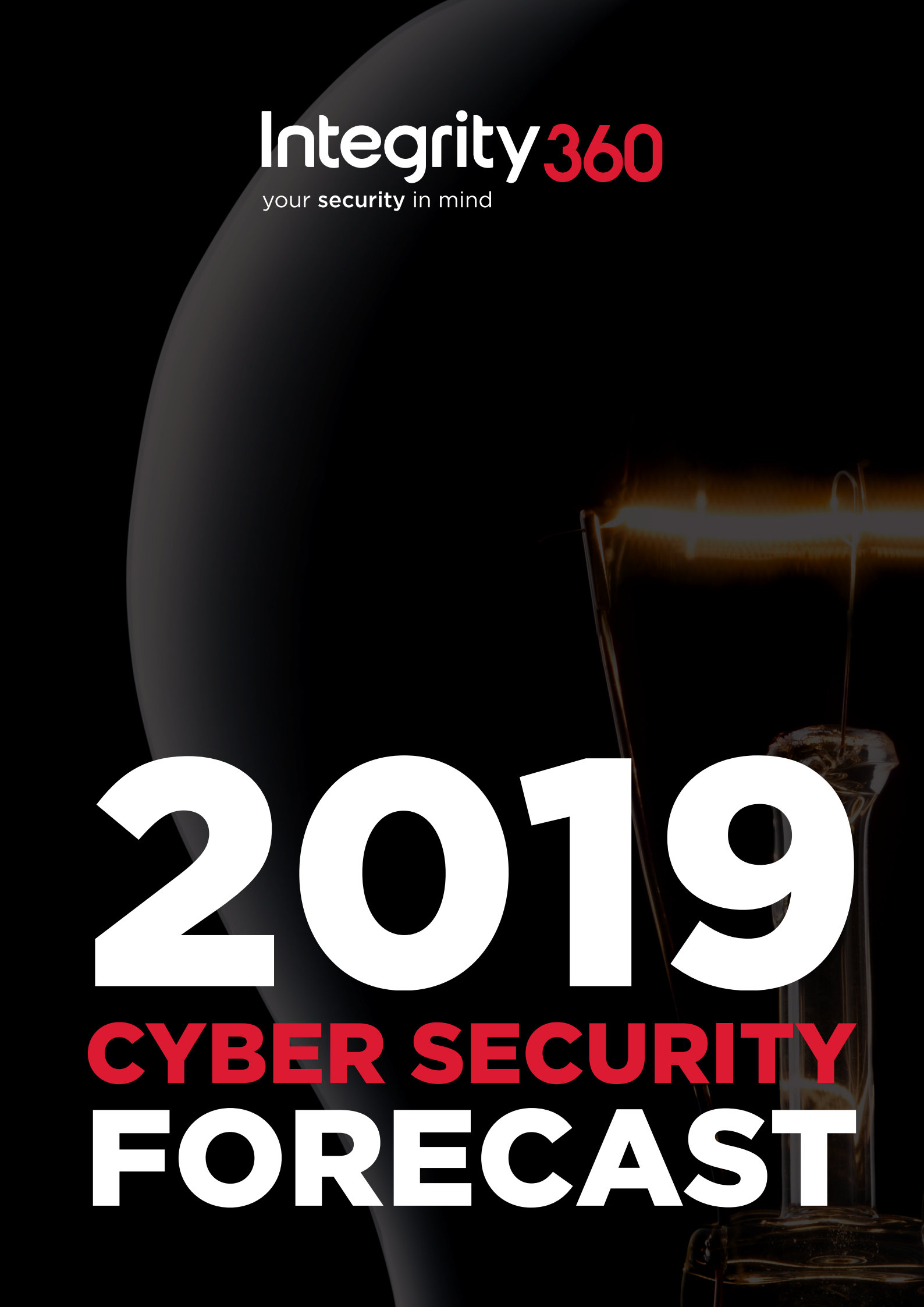
Integrity360

your **security** in mind



2019 CYBER SECURITY FORECAST

Integrity360
your security in mind

CONTRIBUTORS

Richard Ford
Group Technical Director

Sean Rooney
Cyber Risk and Assurance Director

Barbara Pires
Head of Cyber Risk and Assurance

Gavin Schroeder
Head of Cyber Security Testing

Ivan Quill
Pre-Sales Technical Architect

Jamie Davin
Security Consultant

Michael Cowley
Cyber Security Pre-Sales Consultant

Fergal Ward
Security Consultant

Matt Elkington
Senior Security Consultant

Ciarán Johnson
Head of Information Governance

Mike Buckley
Cyber Security Pre-Sales Consultant

Eoin Gilmartin
CRA IT/IS Control Analyst

Introduction

Cyber security specialists rarely got a chance to catch their breath in 2018. The threat landscape shifted multiple times throughout the course of the year as hackers continuously changed their techniques, tactics and targets to stay ahead of companies' security strategies.

Data breaches may have dominated the headlines, but there wasn't a news story as pervasive as the discovery of Spectre and Meltdown earlier in the year.

They wouldn't be the only hardware and firmware vulnerabilities that researchers would find throughout the year, but they served as proof as to just how intricate and far-reaching the exploits could be.

Although there wasn't an event that had the scale of WannaCry, hackers had their time in the spotlight, too. GandCrab hit the scene and released five versions over 12 months, racking up millions in ransom from its victims. Magecart also had great success in breaching the payment infrastructure across a number of big name trusted brands.

The cyber security community didn't take the punches lying down. Countless patches were issued for applications and operating systems. Important frameworks like the CIS Top 20 Security Controls were revised to focus organisations on the basics of security; know your assets, know your software, configure them securely, keep on top of vulnerabilities, protect privileged users and, importantly, carry out proactive security monitoring.

GDPR also made its long-awaited appearance, mandating that businesses take greater control over their data.

Despite everything that took place in 2018, one theme remained persistent:

It's difficult to stay one step ahead when hackers are setting the pace.

But that doesn't mean businesses aren't giving it their best effort. By staying proactive and buying into emerging trends, companies can keep their cyber risk postures on par with best-in-class practices, processes and strategies.

Our experienced teams believe there are eight critically important storylines that every enterprise should know about going into 2019.

Human cyber security

will need to be just as important as technological cyber security

There isn't an umbrella solution for building better cyber security; it's an organisational effort and digital tools only play a part in it. The human aspect continues to be overlooked when it comes to information security governance, but it will need to get more of the spotlight.

People are the first line of defence against the many different types of attacks that cybercriminals launch daily. Developing employee training that's centred on identifying those threats and taking the right precautionary measures should be a primary goal for every business in 2019.

The alternative to a greater amount of security awareness is what we're seeing right now:

> **The human aspect of cyber security continues to be overlooked.**

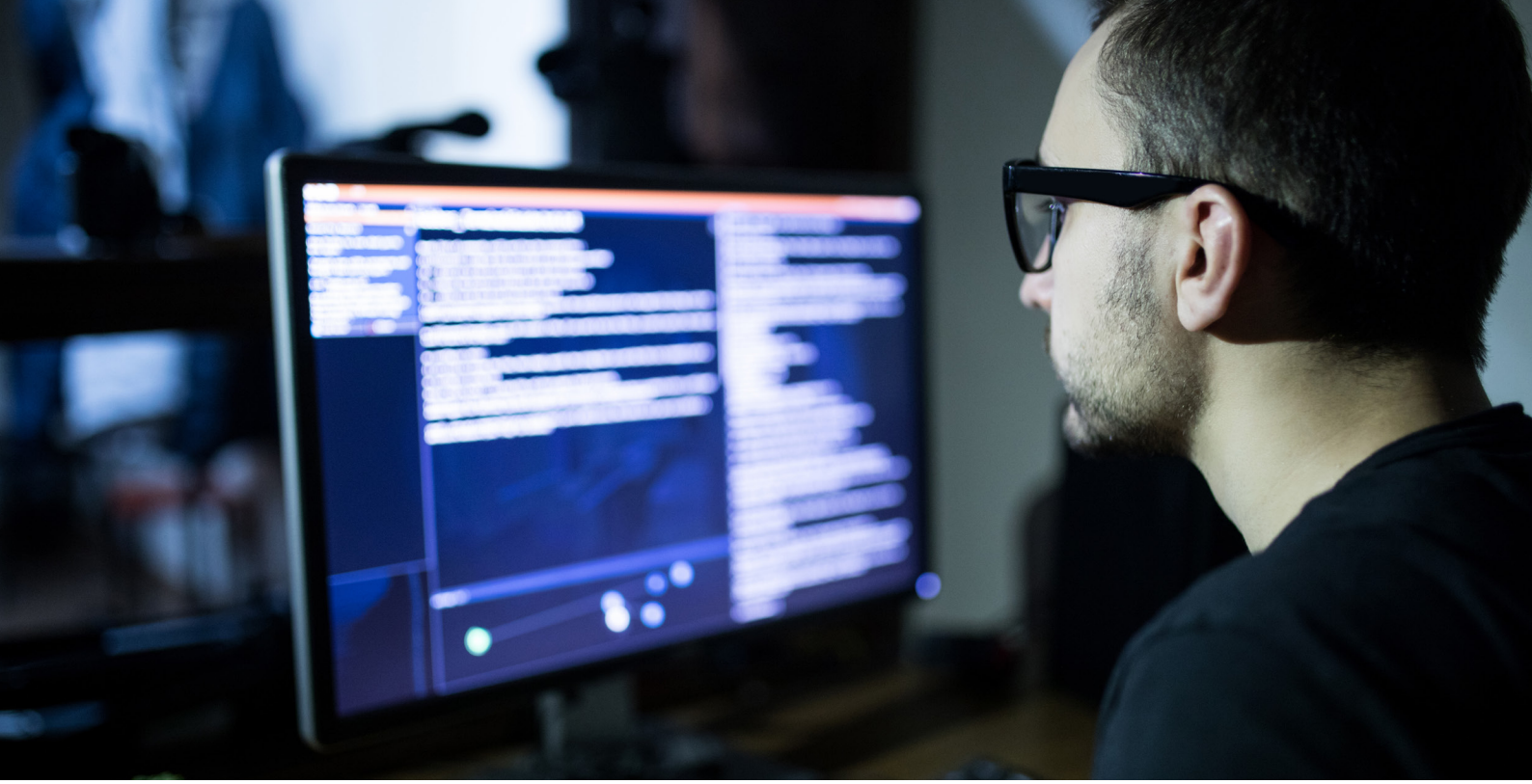
more data breaches. Worldwide, businesses saw cybercriminals compromise 4.5 billion records over the first half of 2018, according to Gemalto.

That's not even counting the latest data breaches at Marriott and Quora, which affected 500 million and 100 million customers, respectively.

Keeping employees aligned with the latest best practices and continuously running exercises to gauge the security awareness programme's effectiveness can have just as much, if not more of an impact as any cyber security tool.

Information security governance is a core function of compliance with GDPR and other regulations, and it isn't just achieved by adopting the latest digital solution. Hackers are using phishing and spear-phishing more commonly now, and there will only be more security incidents down the road if employees aren't able to spot those campaigns.

Investment in cyber security needs to incorporate risk and follow these four steps: People first, then research on the latest trends, then quality cyber security solutions and finally, innovative platforms that keep the company in line with the emerging threat landscape.



Fileless attacks will turn into hackers'

primary method of delivering a payload

As companies' cyber security solutions have grown more intelligent, so have hackers. We've already begun to see a wave of renewed popularity for fileless attacks and there's no reason to believe that will slow down in 2019.

Fileless attacks use legitimate applications like Windows PowerShell to run malicious macros that contact a command and control server to deliver a payload. The method allows threat actors to cut out the middle man – normally an executable file – to boost the chances that they remain undetected.

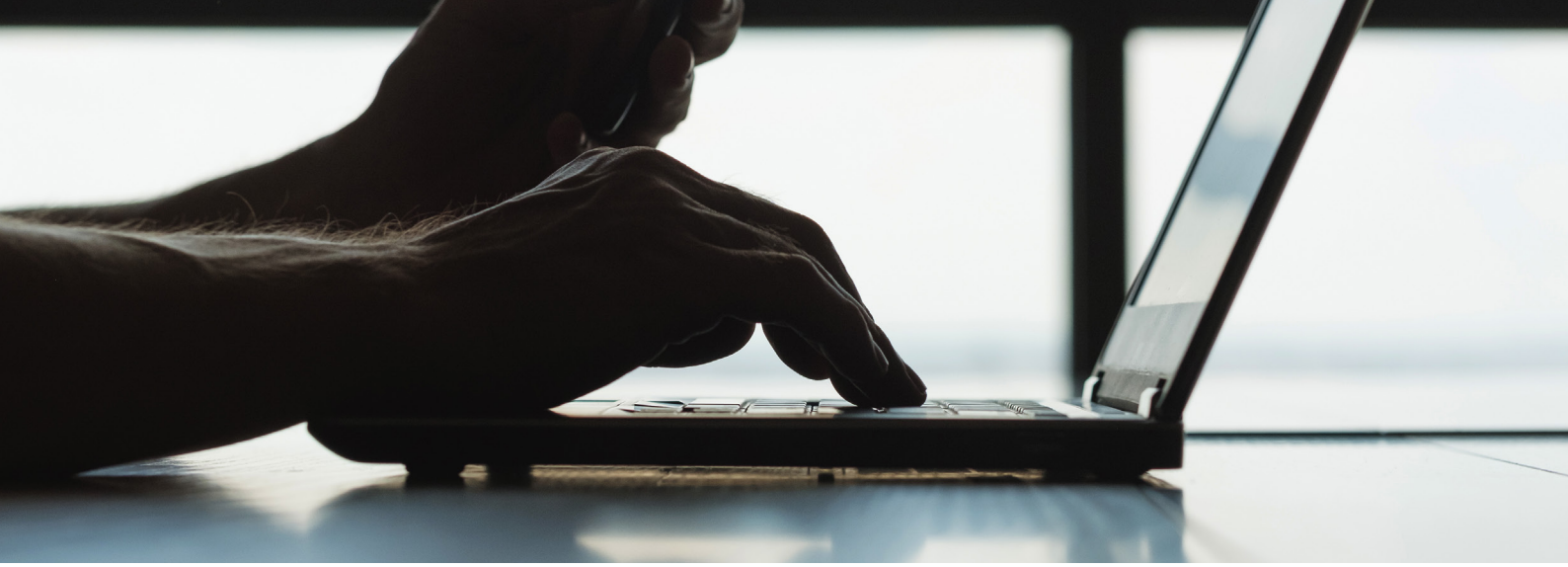
So far, the strategy is working: Over three-quarters of successful attacks in 2017 used the fileless technique, according to a study by the Ponemon Institute. It led to a twofold increase in detections of the attacks over the first half of 2018, from 21.9 detections per every 1,000 endpoints to 42.5, according to SentinelOne.

Emerging cyber security tools that rely on artificial intelligence to detect hacking attempts are better equipped to spot these attempts.

Rather than relying on signatures, which are common with cyber-attacks that use executable files to deliver the payload, the platforms focus on user behaviour. It leads to a far greater likelihood that they can spot an anomaly consistent with a fileless threat.

Of course, not every company's budget is growing as quickly as hackers are innovating. The stagnation is leading to a major gap that's bloating the success rate of fileless attacks.

As long as endpoint security and organisations' security strategies as a whole continue to lag behind, there will be no reason for cybercriminals to fix what isn't broken.



Identity and Access Management

will rightly be seen as an essential part of cyber security

Perimeter-defined security is no longer enough to protect today's digital enterprise. Identity will become the essential core approach to protecting data for customers, partners, employees and devices.

It's easy to be drawn to the latest tools in cyber security and rightfully so – but, don't overlook the fundamental components of a strong cyber risk posture. An identity-defined security approach and Identity and Access Management (IAM) accomplishes a simple task that greatly improves companies' risk mitigation tactics, and it isn't being used enough.

Enterprises will find it essential to closely monitor and manage account and digital device access among all staff, contractors and visitors in 2019.

Companies have been fixated on shortening the time of detection through technology, which certainly has its merits. They've also lost sight of the fact they need to ensure that best-in-class processes and policies are in place if they want to greatly reduce their cyber-attack surface.

IAM has a place in every major initiative that innovative organisations will be undertaking in the new year. Cloud adoption and deployment, container security and compliance with emerging frameworks or regulations all depend on some level of IAM if businesses want to deter cybercriminals.

The companies that are buying into IAM are likely to further their strategies by ramping up their investments and resources into multi-factor authentication and Privileged Access Management (PAM). By association, we'll also see Identity-as-a-Service hit mainstream given its usefulness for providing single sign-on and risk-based authentication services for access in the new digital enterprise.

Moving forward, businesses will need to regularly evaluate the privileges that have been assigned. This shouldn't be done only once a year, or even twice a year, but at least once every quarter on an ongoing basis. Data breaches are attributed to unauthorised access and a startling number of companies are unaware as to which internal members have access to what parts of their systems.

Companies will have to do more

than just the bare minimum to secure the cloud

We're past the point where the cloud is a trend; it's how the modern business operates. Organisations are using it in a variety of ways, especially when it comes to workforce productivity tools like Office 365.

We're on the verge of another cloud trend: cyber security. Enterprises were quick to adopt the solution and have seen the advantages of doing so. But with the focus on DevOps and speed of deployment, many organisations forget the key principle of anything that's connected to the internet - it has to be secure.

Every cloud vendor operates under the shared responsibility model. They protect the infrastructure, and the company using the service is accountable for the security of its data. Within that arrangement lies a common misconception: the servers are configured for security best practices by default.

When a business launches its cloud service, whether it be Azure, AWS or any other platform, the vendor simply makes it operational. It's the responsibility of the end user to bring it and the company's practices in line with their own internal security strategy and any associated regulations.

This is one of the many reasons why we've seen the endless news headlines about data leaks and cloud buckets that were found to be publicly accessible. By leaving default credentials in place and not taking advantage of the built-in security features, enterprises have exposed the personal information of millions of employees and customers over the course of the last year.

It's critical that organisations take the time to evaluate how they'll be using their cloud services and which security controls match best with those associated risks. We're past the point where fundamental tools and policies should be in place for a technology that's been adopted so quickly. Organisations will need to commit the resources necessary to protecting the significant value that proprietary information holds.

Default configurations for the cloud give businesses a false sense of security.

Vulnerabilities within hardware and firmware will continue to emerge

Hackers launching a cyber-attack on a database or persuading users to click a link is one thing; having no control over a device being compromised is a different story.

There's a chance historians look back and dub 2018 as the year of hardware and firmware vulnerabilities. They've always existed, but the scope of what cybercriminals can access has extended greatly over the past year.

Meltdown and Spectre, the zero-day vulnerability that's embedded in the processor of most modern devices, was the first big story to hit the scene this year. Spectre has proven difficult to patch – and likely won't be patched in older machine models – and is a great representation of the problem at large.

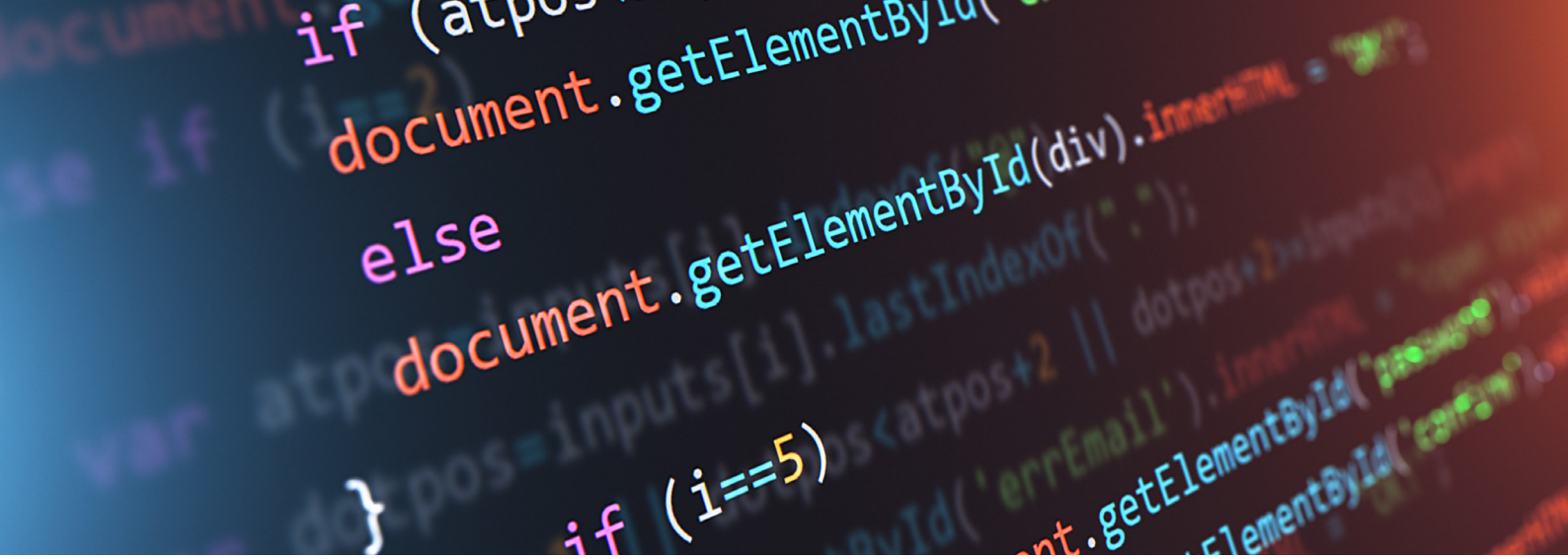
There were also a number of supply chain attacks that entered the public eye. CCleaner, an application that's likely whitelisted on many computers or laptops, was compromised by threat actors who embedded malware in its code. Cyber-attacks that originate from trusted firmware or software is a dangerous evolution and makes it vastly more difficult to stop cybercriminals.

> **There were a number of supply chain attacks in 2018.**

Then there was the revelation that threat actors may have implanted chips that were smaller than the tip of a pencil in Super Micro mainboards to track data and activity inside of servers. It has been repeatedly rebuffed, though not entirely disproven. The story brings nation-state spying to a new level and makes many wonder what other type of hardware alterations are currently in existence which could be unprecedented cyber-threats.

Lastly, we've seen governments begin to recognise the influence of nation-states on the businesses that originate from their countries – and the danger they present to enterprises' cyber risk postures across the world. The trend cropped up with the US government signing into law a ban on agencies using Kaspersky Lab products, then again with countries' resounding rejection of Huawei's proposal to work on the preliminary hardware for mobile 5G networks.

It's uncertain what will happen next in 2019, but there's a growing suspicion that some of the bigger cyber security stories may have more to do with hardware or firmware than they have in the past.



JavaScript code snippets

putting card payment applications at risk

We're now seeing threat actor groups that use a broad range of methods and techniques to launch their attacks, making it more difficult to detect and respond to them on a daily basis.

Even in light of that, one of the most challenging vectors to defend against in 2019 could arguably be known-good JavaScript code snippets and repositories. We all try to find ways of making our jobs easier and hackers have caught on to the fact that software developers avoid reinventing the wheel to implement common functions. Instead, they use either open-source or paid third-party code for projects.

It's not uncommon to lift a few lines of code if it simplifies the task – especially when you'll be writing thousands of lines by the end of the project. That's exactly what hackers are hoping for and they're increasingly beginning to exploit it by leaving malicious code in highly targeted areas of the web.

Repositories like GitHub are well known for their usefulness, providing software developers with code that would otherwise take them hours to create. But hackers are able to compromise it with just a few extra lines that are difficult to spot unless a technical engineer knows exactly what to look for.

Furthermore, the malicious code may not even be on your website and instead be served via the compromised third party. In the case of the Feedify data breach, this meant that customers not only received the push notification capability by linking to the hosted JavaScript, but also unwittingly the added Magecart exploit code – giving attackers instant access to a large number of end users.

Where JavaScript is being directly hosted, attackers are modifying known-good third-party scripts to tack on their malicious actions, making it extremely difficult to spot.

Magecart and payment skimming aren't the only threats. JavaScript helps hackers deliver a wide range of attacks. One example is that malicious JavaScript running on compromised websites lets attackers exploit the Meltdown vulnerability if it hasn't already been patched on the machine. This gives hackers full access to the user's cached data.

DevOps and Agile Development has undoubtedly been a benefit for software developers, but the speed in which edits and upgrades are made can lead to mistakes and also make it hard to spot malicious activity and changes.

Assuming JavaScript, either publicly available on GitHub or acquired via a trusted third party, is legitimate may lead to technical engineers unknowingly compromising their company's cyber security.

Companies will slow down security deployments and take their foot off the pedal of DevOps

We've reached an inflection point with DevOps. DevOps has had a profoundly positive impact on business' ability to deploy technological solutions quickly and efficiently, but it's moving at a speed that's too fast for many security teams to keep up with.

Companies will have to embrace new ways to deploy security tools in 2019. The addition and subsequent growth of DevOps teams has allowed organisations worldwide to remain agile. However, it has put more infrastructure decision-making power in the hands of DevOps; taking it away from infrastructure and network security functions. DevOps are often now in control of which building blocks are used and how and when these are deployed within an organisation.

In doing so, many of the traditional checks and balances that ensure business' digital environments remain safe and secure are being overlooked.

It is clear that nowadays the fully-engineered "build and test" approach does not meet many businesses time-bound expectations. Most modern projects are built with massive scale and speed to market in mind; requiring deployment to thousands of devices in a matter of hours and minutes, rather than weeks and months. Combining this aggressive and agile DevOps approach with the huge scale and reach of cloud services, businesses now face new challenges. Their security landscape and cyber risk profile can dramatically change with the click of a button and the deployment of new code or supporting infrastructure.

There will need to be a major paradigm shift in the way in which businesses provision security solutions in 2019. Secure code will need to become part of the culture and approach of organisations. Scanning and assessment of applications and code on creation, rather than on deployment, should be promoted as the 'norm'.

DevOps won't go away – nor should it – but businesses will start to understand that it isn't synonymous with cyber security. DevOps makes it challenging to pin down the true stakeholders who make decisions on changes that affect the risk posture of the entire company. It doesn't mean they can't co-exist, and companies will spend a great amount of time figuring out how they can work together more effectively in the new year.

Artificial intelligence

will be critical for hackers and companies alike

The age of automation is made possible in part thanks to artificial intelligence, which is now at the forefront of cyber security. At the same time, hackers haven't let its usefulness pass by unnoticed.

Researchers believe that cybercriminals who are able to truly use artificial intelligence to their advantages will ultimately produce much more effective cyber-attacks – a worrying thought for any business. Once this happens, basic tools and elementary strategies will struggle to keep pace with the rapid evolution of cyber security.

Artificial intelligence will enable hackers to develop stronger attacks that leverage critical zero-day vulnerabilities and get their campaigns through defences largely undetected, according to a report titled, "The Malicious Use of Artificial Intelligence."

Spear phishing, social engineering and malware attacks are all expected to see an uptick in success rates as artificial intelligence will allow cybercriminals to expertly craft their attempts and hone in on vulnerable components of an organisations.

Cyber security won't be overmatched, though. Vendors are introducing artificial intelligence in a variety of ways to improve their products and services.

Endpoint security, for instance, commonly relied on pre-baked signature detection for years to spot attacks. Now with artificial intelligence, certain platforms can detect a cyber-attack based on a wide range of indicators of compromise – even when they're not connected to the internet.

Artificial intelligence has also made its way into SIEM, using machine learning to build a baseline of normal behaviour, at both the user and asset level, identify deviation. In doing so, it's able to provide businesses with an exhaustive view of their environment's security, improve its chances of detection and cut down on false-positive notifications.

Artificial intelligence has been a buzzword for some time, but now we're seeing tangible improvements in its usefulness for cyber security. Unfortunately, cybercriminals are too.

Hackers and companies are both using AI.

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 (0)1 293 4027

LONDON OFFICE
90 Long Acre,
Covent Garden, London, WC2E 9RZ
+44 203 397 3414

BIRMINGHAM OFFICE
TS2 Pinewood Business Park,
Coleshill Road, Birmingham, B37 7HG
+44 203 397 3414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1 212 461 3286

WWW.INTEGRITY360.COM

Integrity360

your **security** in mind