



CYBER SECURITY RISK RADAR

CONTENT

- 2** Executive summary
- 4** Multiple companies fined for their role in data breaches
- 5** Cyber-attack spotlight heats up for financial sector
- 6** Third-party vulnerabilities exploited in Facebook data leaks
- 7** The data breach decade keeps rolling on into 2019
- 8** New SplitSpectre vulnerability easier to carry out than Spectre
- 9** Intel reflects on a year of progress with Spectre and Meltdown
- 10** GandCrab enters version 5 but a decryptor is released
- 11** WannaMine spreads through companies using EternalBlue exploit
- 12** Cryptomining attacks surge in popularity in 2018
- 13** Ransomware-as-a-Service sustains financial success
- 14** Cisco tries to patch major WebEx vulnerability
- 15** Kubernetes cloud container hit with first critical vulnerability
- 16** Microsoft adding sandbox capability to Windows 10
- 17** Multi-factor authentication adoption on the rise
- 18** Employees continue to be Achilles' heel in cyber security strategies
- 19** Quarterly Report Spotlight: RiskIQ and Flashpoint

Executive summary

The fourth fiscal quarter of 2018 saw developments on nearly every front in cyber security. Data breaches, ransomware and vulnerabilities dominated the headlines. Here's what you need to know:

- ✓ A number of **businesses were fined for how they handled data breaches**, which includes a German privacy regulator handing out its first GDPR fine.
- ✓ The **financial sector is seeing an uptick in data breaches**, and the securities market is most at risk.
- ✓ Facebook dealt with **multiple data leaks stemming from its third-party data security** policies.
- ✓ Early estimates show that **2018 was one of the worst on record for data breaches**. Though it still lags behind 2017.
- ✓ The SplitSpectre variant was revealed, which is essentially **an easier way to attack the Spectre vulnerability**.
- ✓ Intel revealed the **strides it's making in mitigating Spectre and Meltdown**, as well as its plans for securing hardware in the future.
- ✓ GandCrab development entered version 5, but **Bitdefender created a decryptor for versions 1, 4 and 5**.



- ✓ Cryptojacking campaign **WannaMine is using the EternalBlue exploit to spread** through networks, similar to the WannaCry attack.
- ✓ Hackers are switching to cryptomining in droves as **the volume of cryptojacking attacks jumps 83 percent** year-over-year.
- ✓ **Ransomware-as-a-Service is proving to be a lucrative business**, which should have companies worried.
- ✓ Cisco had to patch a vulnerability in WebEx twice this last quarter, **reinforcing the need for continual patch management**.
- ✓ Researchers discovered a **critical vulnerability with the popular Kubernetes** cloud container orchestration platform.
- ✓ Microsoft aims to release **a built-in sandbox for Windows 10 Pro and Enterprise users** so they can run executable files in a virtual instance.
- ✓ **Adoption rates of multi-factor authentication are rising** as new solutions hit the market, with smaller companies leading the way.
- ✓ A survey shows that **three out of every four employees pose a risk** to their company's data security strategy.



Multiple companies fined for their role in data breaches

UK and Dutch regulators handed Uber a combined £900,000 fine for its role in the data breach that compromised customer and driver information in 2016. Elsewhere, Italian regulators gave Facebook a €10 million fine for breaching the country's consumer privacy policy and misusing customer data.

A German data protection agency, Baden-Württemberg DP Authority, handed out its first GDPR fine to Knuddels, a dating and chat website. The company was ordered to pay €20,000 for its lack of effective security controls regarding a data breach that compromised the information of over 330,000 users.

360 Insight

Data protection authorities are cracking down on businesses that show a clear disregard for protecting customer data. In the case of Knuddels, the website stored passwords in plain text making it easy for a cybercriminal to extract the information once gaining a foothold.

The fines are a sign that regulators expect organisations to take ownership over both the security controls they have in place and their incident response plans. Uber reportedly tried to cover up the data breach by paying off the cybercriminal, which resulted in more fines, settlements and legal trouble than simply reporting the breach might have brought on.

Multiple companies were fined for how they handled their security incidents.

Cyber-attack spotlight heats up for financial sector

Enterprises in the banking and financial services sectors reported 103 data breaches over the first half of 2018, according to Bitglass researchers. This is a 278 percent increase over the data captured just two years ago during the first half of 2016.

At the same time, researchers believe the securities markets and payment facilitators are more vulnerable to immediate cyber-threats than traditional banking services, according to SWIFT. This is attributed to their complex organisational structure, sprawling number of endpoints and loosely secured communications channels.

360 Insight

While cyber-attacks in the financial sector are commonly associated with banks, research suggests that cyber security specialists should be looking elsewhere in the industry. Cybercriminals thrive on poor security controls and the sometimes chaotic daily operations of securities markets can be a breeding ground for them.

Cyber security should be a major priority at all financial institutions given the sensitive nature of the Personally Identifiable Information (PII) that those companies handle. It is for the most part, but knowing that they have a target on their backs should encourage them to continue to seek out best-in-class solutions to fend off attacks.

Banks and financial services saw 103 data breaches take place in the first half of 2018.

Third-party vulnerabilities exploited in Facebook data leaks

Facebook earned a spot in the news cycle for three different data leaks that compromised over 118 million users combined. A large portion of the PII is suspected to have been used for a social engineering campaign.

The largest data leak totalled roughly 87 million users. Access to their profiles was gained through a third-party application. Three in every five companies have experienced a security incident stemming from a third-party service and only one-third of businesses have an exhaustive inventory of their vendors, according to a study by The Ponemon Institute.

360 Insight

The result of the Facebook data leaks is less interesting than how they happened in the first place. Facebook's relaxed data security policies coupled with a lack of focus on third-party access allowed malicious groups to take advantage and scrape the personal information of millions of users.

It's clear that companies continue to overlook third-party vendors and the access they have to proprietary data. It's a misstep, as those same businesses are still responsible for how that information is stored, accessed and used – and it can land them in trouble with GDPR if a breach takes place.

Three different Facebook data leaks compromised the information of over 118 million users.

The data breach decade keeps rolling on into 2019

Although it lags behind the figures of 2017, Risk Based Security researchers estimate that 2018 will finish as one of the worst ever for enterprise data breaches. The report noted that nearly 3,700 breaches compromised over 3.6 billion records through the end of Q3 2018.

Since then the cyber security community has learned of the Marriott hotel chain data breach (383 million records compromised), Quora's (100 million records), Cathay Pacific (9.4 million records) and countless others.

Hackers accessed over 3.6 billion records just three-quarters of the way through 2018.

360 Insight

The past year shows enterprise cyber security is slightly improving as the total number of breached records doesn't come close to the 7 billion compromised in 2017. However, the world still saw data breaches or leaks that affected 1.1 billion users (Aadhaar), 383 million records (Marriott) and 340 million consumers (Exactis).

It will only become more difficult to safeguard PII from cybercriminals as their options and techniques expand. Businesses can keep pace with the emerging threat landscape by ensuring their cyber security strategy is aligned to a framework and by adopting best-in-class tools.

New SplitSpectre vulnerability easier to carry out than Spectre

Researchers revealed a new exploit for the Spectre vulnerability, named SplitSpectre. The cyber-attack is reportedly easier to execute than the original Spectre attack. Essentially, hackers wouldn't need to place a device near the target to conduct a cyber-attack with SplitSpectre.

SplitSpectre was successfully launched against a few Intel and AMD processors that hadn't patched the vulnerability via Mozilla Firefox's JavaScript engine, SpiderMonkey. It would theoretically be viable against all processors that were vulnerable to the original Spectre.

SplitSpectre is a new variation of the original Spectre exploit.

360 Insight

Spectre opened the year along with Meltdown as two of the most powerful hardware exploits in the right hands. Since then, multiple variants of the two have been identified and a number of patches have been created to mitigate the vulnerabilities.

While SplitSpectre was just found, it can't be executed on devices that have taken the necessary precautions to defend against the original Spectre. These include patches for operating system updates released by manufacturers as well as patches for browsers from which the attacks can be launched.

Intel reflects on a year of progress with Spectre and Meltdown

Intel gave a glimpse into the efforts its researchers and internal teams have made to secure end users from the Spectre and Meltdown exploits over the course of 2018. The company aims to build security features into the architecture of all hardware from the 8th generation of processors on.

At the outset, Intel created the Intel Product Assurance and Security (IPAS) group to provide security and quality support across the business. The company also aims to package microcode for Spectre into regular Windows updates and commit to more frequent red team exercises.

360 Insight

While the Intel camp wasn't completely silent over the last year, little information was publicly available as to how the company would stop another Spectre or Meltdown from cropping up again. Intel's editorial cast a spotlight on the significant changes it's making in light of the discoveries.

Patch management plays an intricate role in protecting users from the Spectre and Meltdown side-channel cyber-attacks. Ensure your business is regularly applying patches, especially those delivered by Original Equipment Manufacturers (OEMs) for their hardware.

Intel is packaging Spectre and Meltdown patches with routine Windows updates.

GandCrab enters version 5 but a decryptor is released

The creators of GandCrab maintained the ransomware's rapid evolution by releasing version 5. The developers improved its ability to encrypt files on shared network drives and struck a partnership with NTCrypt to better obfuscate its code.

During the same time, Bitdefender worked with a number of international agencies to release a decryptor for GandCrab. The tool helps victims get back their files free of charge, but only works for version 1, 4 and 5.

360 Insight

The decryptor tool is a welcome sign for the cyber security community. GandCrab is notorious for its quick development but also its ability to overcome decryption tools. Its developers continue to branch out and add new features and techniques to evade detection.

GandCrab capitalises on two Common Vulnerabilities and Exposures (CVEs) in particular: CVE-2018-8440 and CVE-2018-8120, according to McAfee researchers. Businesses should ensure these vulnerabilities are patched and that anti-ransomware and endpoint security tools are always running.

The GandCrab decryptor works for versions 1, 4 and 5.

do your need?
ed GandCrab Decryp
oftware will decrypt al
urchase you need cryp
o buy this currency yo
ow much money you

Xq34

This process is fully a
ment p

WannaMine spreads through companies using EternalBlue exploit

Researchers continue to see a steady uptick in WannaMine detections over the past few months. The fileless cryptominer is similar to WannaCry in that it spreads throughout a network by using the EternalBlue exploit.

Although the patch for EternalBlue has existed since March 2017, many businesses have yet to update their systems. WannaMine uses PowerShell to deliver its payload, though it does leave behind a large file on the machine afterward.

360 Insight

The fact that WannaMine is picking up steam while relying on EternalBlue shows that businesses are ignoring the lessons learned from the WannaCry and NotPetya cyber-attacks. Patching EternalBlue or any other CVE will ensure the company can't become a victim to WannaMine or similar threats.

Cryptomining victims are commonly associated with consumers but cybercriminals are increasingly looking towards large corporate networks as a way to stay hidden and generate a substantial return. CrowdStrike researchers reported that some organisations hit with WannaMine have seen operations stop from anywhere between days or weeks at a time.



WannaMine takes advantage of EternalBlue to infiltrate corporate networks.

Cryptomining attacks surge in popularity in 2018

The number of cryptomining attack victims over the first three fiscal quarters of 2018 increased nearly two-fold over the same stretch during 2017. Kaspersky Lab researchers revealed that over 5 million instances were identified through Q3 2018, compared to just 2.7 million the year before.

The 83 percent increase in volume doesn't come as a surprise as cryptomining activity loosely followed the ebb and flow of the price of Bitcoin, according to the report. McAfee researchers saw the number of cryptomining variants grow 4,467 percent over the course of 2018.

360 Insight

Cryptomining can be just as profitable if not more so than ransomware. Large-scale cryptomining operations aimed at infiltrating corporate networks are difficult to detect and can significantly reduce the performance of systems that are critical for daily operations.

Organisations should enforce networking and security best practices to avoid becoming a victim to cryptomining. Segmenting the network and adopting endpoint security that relies on behaviour-based detection are two ways that businesses can protect themselves from the cyber-threat.

Cryptomining offers the near-instant payout that ransomware can't.



Ransomware-as-a-Service sustains financial success

Researchers believe that GandCrab's Ransomware-as-a-Service platform netted its developers an estimated \$300 million over the second half of 2018. The customisable ransom notes and price demands are a major reason behind its success.

Kraken Ransomware-as-a-Service requires users to pay \$50 to become an affiliate member, as well as hand over one-fifth of the ransomware payment to the developer. The service has only been available since the end of Q3 2018, but it has already been used against hundreds of victims.

360 Insight

Skilled hackers have found out they can make more money by offering their ransomware or malware as a service, rather than conduct the attacks on their own. This gives them a degree of separation while still benefitting financially.

In turn, Ransomware-as-a-Service makes it much easier for the average hacker to carry out an attack and makes the malicious threats more prevalent than they might have been in the past. Companies should already have multiple tools in place to detect and prevent ransomware infiltration.

Ransomware-as-a-Service is profitable for affiliates and developers.

Cisco tries to patch major WebEx vulnerability

Cisco tried unsuccessfully to patch a vulnerability within its WebEx conference platform in October, leading to a follow-up patch being released in late November. The exploit can be used against platforms running on version 33.6.4 and lower.

The vulnerability would allow attackers to issue commands with administrative privilege when exploited, though the hacker would likely need local access to execute it. Note that cybercriminals can still launch the attack through an Active Directory user's remote management tools.

360 Insight

Cisco's WebEx wasn't the only conferencing tool to come under scrutiny for a vulnerability in Q4 2018, as an exploit was found for Zoom too. Although, it does serve as a shining example of why it's important to stay on top of patching.

Had a business updated its software without continuing to keep track of the story, they might find themselves still vulnerable at this very moment. Patch management strategies should be consistent and ongoing to ensure exploits are entirely mitigated.

A number of vulnerabilities were found in conferencing tools in Q4 2018.



Kubernetes cloud container hit with first critical vulnerability


A critical vulnerability was found for Kubernetes, the widely used open-source cloud container orchestration platform. The CVE scored a 9.8 out of 10 on the Common Vulnerability Scoring System (CVSS) for its ease of application and its severe impact.

The exploit lets attackers send authenticated requests through the Kubernetes' API to gather data and modify the code that's hosted in the particular container. The vulnerability effectively gives hackers administrative control over the environment.

360 Insight

The Kubernetes exploit is critical because it allows hackers to conduct a wide range of actions with little resistance. Furthermore, logs won't pick up those actions as the requests are sent over a legitimate, authenticated connection.

There is good news: the vulnerability only affects Kubernetes environments running version 1.0 – 1.9. If your organisation is running a later version it will be safe from the exploit, and if it's running an earlier one then it needs to upgrade as soon as possible.



Hackers can send authenticated requests with the Kubernetes vulnerability.

Microsoft adding sandbox capability to Windows 10

Microsoft is expected to debut its Windows Sandbox feature in 2019 on its Windows 10 Pro and Enterprise operating systems. The application will allow users to run an executable file through instanced versions of Windows 10 to evaluate its legitimacy.

The sandbox will be a lightweight virtual machine that most modern systems will be able to run. Apart from isolating the kernel and ensuring the program in question can't affect the machine, it's uncertain what types of cyber security features the tool will offer.

Every user will soon have access to a cyber security sandbox.

360 Insight

Microsoft's announcement of its Windows Sandbox is a sign that the general view on a sandbox has shifted from it being a useful tool to it being an essential one. Every user having access to a built-in sandbox should help reduce the success rate of phishing and similar campaigns.

No two sandboxes are the same, despite all of them being tasked with the same function. It's currently unknown how effective Microsoft's sandbox will be, and companies should be aware that it might not be a solution that's up to par with what's required in a cyber security strategy.

Multi-factor authentication adoption on the rise

Multi-factor authentication (MFA) adoption is on the rise across the world. Roughly 45 percent of companies use it in some capacity, according to a study by LastPass. The technology and software industry boasts the highest adoption rate at 31 percent, with banking and finance trailing behind at 16 percent.

This year's findings are a 20 percent jump over last year's. MFA usage was strongest among companies with between one and 25 employees at 41 percent, while companies with 1,000 to 10,000 employees checked in with just a 9.1 percent.

360 Insight

Password security remains a chief concern within enterprises; around half of all employees reuse passwords or only change them slightly, according to a study by Virginia Tech. MFA gives businesses a failsafe to reduce the chance that an account is compromised by phishing or other means.

Organisations like Microsoft and Google are pushing for biometric, passwordless and Universal 2nd Factor authentication to enhance account safety while keeping their adoption simple. Even with MFA in place though, companies must remain vigilant as hackers are now bypassing MFA with automated phishing toolkits.



MFA is a fundamental security tool, but adoption still trails in banking and finance.

Employees continue to be Achilles' heel in cyber security strategies

The workforce continues to clash with companies' goal of better data security, according to a study by MediaPRO. It found that 75 percent of employees pose a risk to the business' customer and proprietary data security, which was an increase over last year's figures.

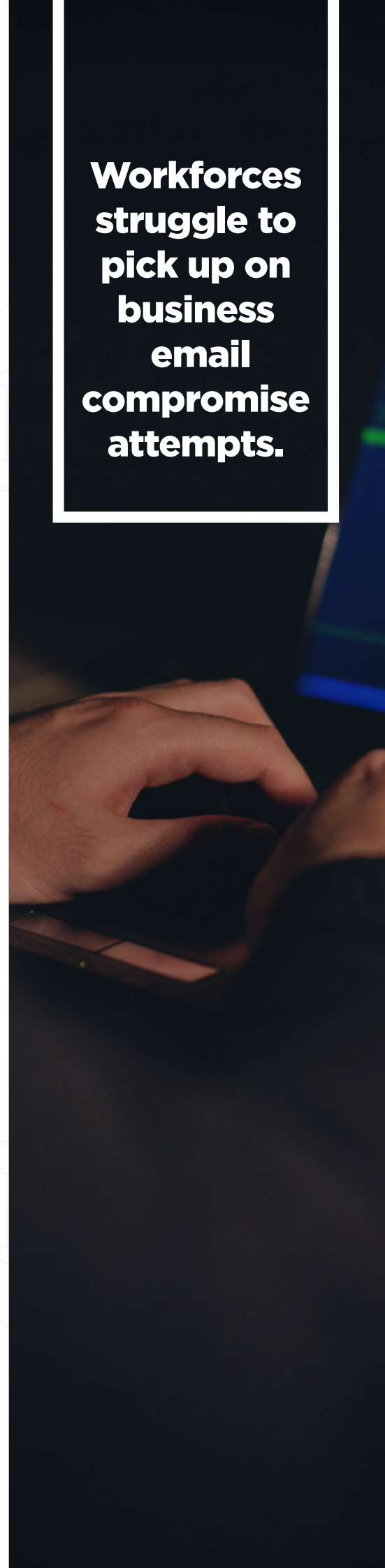
Employees fared poorly when it came to business email compromise, with just 42 percent able to identify it. On the other hand, 86 percent of respondents were able to spot phishing emails. The financial sector's workforce scored the worst out of the eight major industries.

Workforces struggle to pick up on business email compromise attempts.

360 Insight

Employee awareness training has always been crucial to the integrity of an organisation's data security strategy. Unfortunately, data shows that it's either not as effective as it needs to be or that companies are doing away with it altogether.

An organisation's staff is its first line of defence against many of the techniques that hackers are using today. Human security is just as important as digital, and security awareness training should be as high of a priority as any other component of a cyber security strategy.



Quarterly report spotlight:

RiskIQ and Flashpoint

There's never a dull moment in the cyber security industry, and the reason behind that is the great work being done behind the scenes to bring important issues to the public spotlight.

RiskIQ and Flashpoint's Inside Magecart report explores the malicious threat actors behind the high-profile breaches of Ticketmaster and British Airways, among others. Researchers reveal that Magecart is composed of at least six different groups, with each having its own way of operating.

The report includes:

1. The origins of Magecart.
2. Detailed breakdowns of the activity and calling cards of Groups 1 through 7.
3. Related unclassified threat groups.
4. Sales of the stolen cards on the Dark Web.
5. Magecart's method of mule-handling and shipping goods using stolen credit cards.
6. Disrupting the Magecart activities.
7. Indicators of Compromise associated with Groups 1 through 7.

You can read the entire [Inside Magecart report here](#) ➔

RiskIQ and Flashpoint revealed that Magecart is made up of multiple groups.

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



Integrity360
your **security** in mind