CYBER SECURITY RISK RADAR

CONTENT

2 Executive summary

4 Economic downgrade, bankruptcy tied to data breaches

5 Companies pay the piper to remediate data breaches

6 GandCrab closes up shop as decryptor is released

7 Ransomware payouts rise twofold

8 Enterprise trojan detections rise 650% year-over-year

9 Emotet botnet dominates email malware in Q1 2019

10 Office 365 fails to stop 25% of phishing emails

11 Exposed data up 50 percent due to misconfigurations

12 Employees sharing sensitive information via email, IM

13 Microsoft scraps its password reset policy

14 FIDO2 certifications get Microsoft closer to passwordless world

15 Spammers using Google Services to deliver campaigns

16 Google reveals it stored passwords in plaintext

17 Thousands of websites compromised in supply-chain attack

18 Intel reveals ZombieLoad vulnerability in modern chips

19 Quarterly report spotlight: Verizon

Integrity360
your security in mind

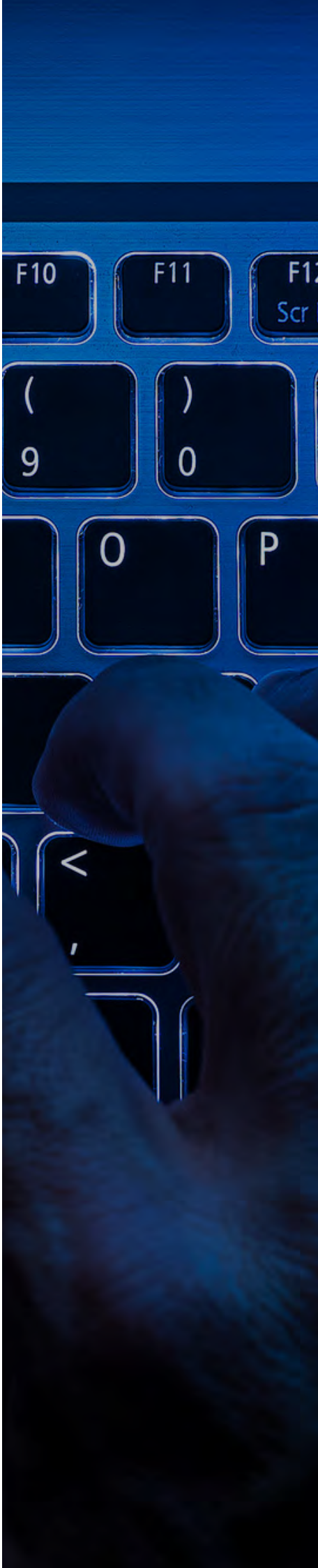
JULY 2019
Q3

Executive summary

The second fiscal quarter of 2019 saw the reign of GandCrab ransomware come to an end, enterprise trojans came back into the spotlight and data breaches caused companies financial havoc. Here's a quick roundup of everything you need to know:

- Equifax became the **first company to receive a rating downgrade due to a breach** as the ramifications of a security incident enters the spotlight.
- Eddie Bauer, Yahoo and Equifax **faced the financial fallout from settlements and remediation** relating to their data breaches.
- The operators behind **GandCrab ransomware announced they would shut down the service** but not before a decryptor was released.
- **Ransomware payout has risen nearly twofold** thanks to more sophisticated variants that allow for larger, high-value targets.
- **Enterprise trojans are on the rise** as hackers look to hide their malware behind seemingly innocent processes, hoping to evade detection.

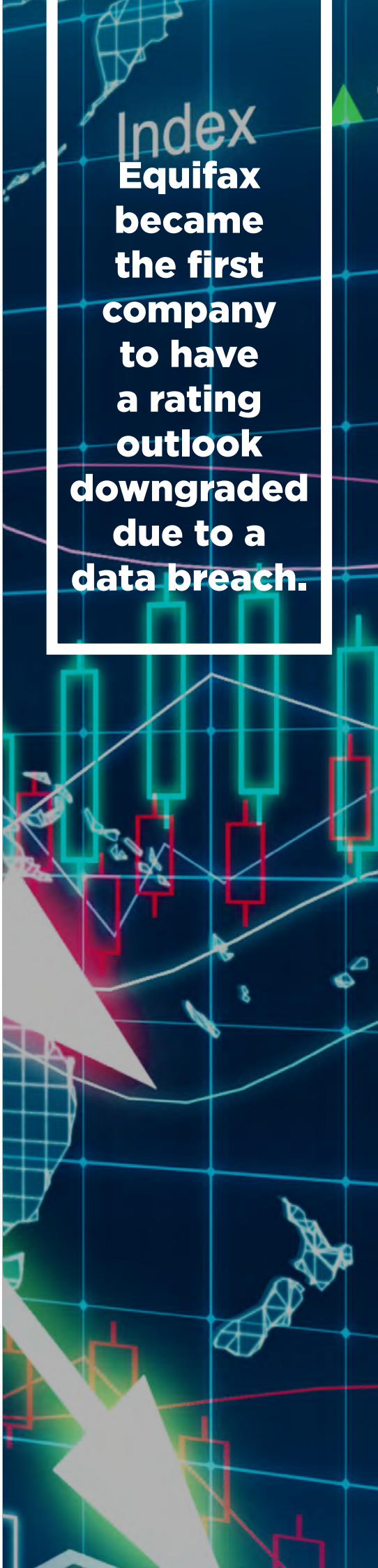
- Researchers found that botnet activity is on the rise and running rampant in email malware, with **the Emotet botnet leading the way.**
- Office 365's basic email security tools **fail to stop 25 percent of phishing emails**, which end up reaching the end user.
- A **50 percent uptick in exposed sensitive data** is tied to the slew of misconfigurations within Office 365 environments and Amazon S3 buckets.
- One study found that **employees are increasingly willing to share sensitive information** via email and IM.
- Employees won't be asked to change their passwords by default anymore, as **Microsoft scraps its 60-day password reset policy.**
- A passwordless future is on the horizon as **Microsoft gets FIDO2 certification for its Windows Hello** biometric-security feature.
- Spammers are **taking advantage of the interconnected Google Services ecosystem** in order to deliver their campaigns.
- Google announced that a small portion of its G Suite enterprise customers **had their passwords stored in plaintext.**
- Hackers hosted malicious code on seven third-party vendor websites in order to **compromise thousands of customer websites.**
- **ZombieLoad was revealed to be a vulnerability** found in all Intel chips created since 2011, allowing hackers to extract data from a device.



Economic downgrade, bankruptcy tied to data breaches

Credit rating firm Moody's recently downgraded the rating outlook of Equifax due to its 2017 data breach. Equifax became the first company ever to see its rating outlook downgraded over a breach. Moody's cited mounting expenses from the breach and significant infrastructural investments in security needed in the future as reasons for the downgrade.

Elsewhere, the American Medical Collection Agency filed for bankruptcy after a data breach that exposed data on roughly 20 million Americans. The company cited its four largest clients ceasing business with it as the main reason behind the bankruptcy filing.



Equifax became the first company to have a rating outlook downgraded due to a data breach.

360 Insight

These two events serve as a reminder that although confined to the digital space, data breaches can have very real consequences. A single breach carries enough influence to result in a rating's downgrade – a significant sign for investors – or a company shuttering altogether.

Avoiding a data breach and the fallout that comes with it has earned itself a seat at the table of the board of directors. Without making investments into the digital security of the business, an enterprise could soon find itself left with a very long bill.

Companies pay the piper to remediate data breaches

A slew of companies saw the financial ramifications of data breaches come to light over the past quarter. Eddie Bauer, a retail company, and Yahoo both agreed to settlements over data breaches that exposed customer data. Eddie Bauer paid $9.8 million to settle and Yahoo offered $118 million.

News came to light that Equifax had paid roughly $1.4 billion so far in the wake of its 2017 data breach that saw the information of 148 million people exposed. The costs are attributed to remediation and ongoing security strategy improvements, and are having an impact on the company's bottom line.

360 Insight

Eddie Bauer, Yahoo and Equifax are all serving as great examples of how much a data breach can really hurt. Apart from initial recovery and remediation costs, or ongoing expenses tied to improving a cyber security strategy, companies that suffer a security incident also see their coffers drained via lawsuits and ancillary costs.

The fact that many of these expenses are coming years down the line shows that a single data breach can have a financial impact reaching anywhere between two to seven years, depending on the severity of it.

GandCrab closes up shop as decryptor is released

The creators behind the popular Hacking-as-a-Service ransomware, GandCrab, notified its customer base that it would be shutting down the operation by the end of June 2019. The developers boasted that GandCrab brought in $2 billion in its lifetime, with the creators taking home $150 million.

Shortly following that announcement, a decryptor for all versions of the ransomware was released. The joint venture between Bitdefender, the FBI and Europol resulted in the first decryptor that can unlock files in all versions of GandCrab.

360 Insight

GandCrab has made an appearance in every publication of the Risk Radar since its inception given its expansive reach and agile development techniques. There are questions surrounding whether it will actually shut down and it's likely that even if it does go offline, something will take its place.

The ransomware was seen as an enterprise venture for its creators and if it were a legitimate company, it'd likely be seen by investors as a unicorn. It goes to show how profitable these advanced operations can be when next-generation antivirus and spam filtering are not effectively deployed.

Ransomware payouts rise twofold

The average ransomware demand has risen nearly twofold in 2019, according to researchers at Coveware. Where the average incident resulted in a payout reaching roughly $6,700 in Q4 2018, victims paid out an average of almost $12,800 per incident in Q1 2019.

The rise in compensation is attributed to a couple of different elements. The most notable of which is the improved sophistication in families of ransomware like Ryuk, which is commonly used to target cities for payouts that reach roughly $286,000 on average.

The average ransomware payout has doubled in 2019.

360 Insight

While operators like those behind GandCrab have made ransomware more accessible, there's another segment of the hacking population that's working to make ransomware more advanced than ever before. The latter is producing cyber-attacks that cripple key infrastructure and cause widespread damage.

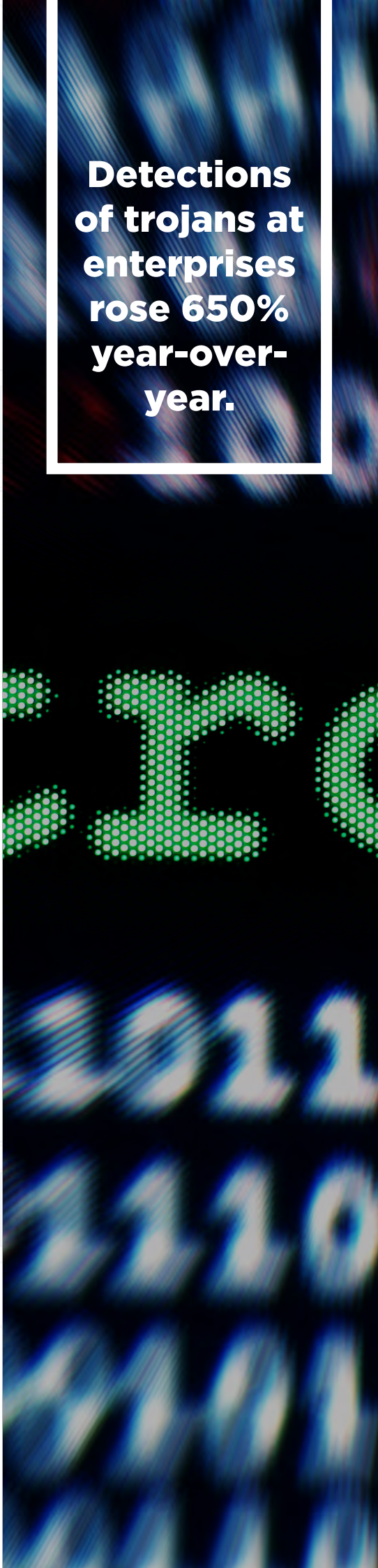
In light of these recent developments, deployments of next-generation antivirus tools should be a given and the value of a proactive cyber security strategy needs to be recognised by company boards. Apart from the rise in payout costs, a security incident was also found to last up to a week on average, which can harm business continuity.

Enterprise trojan detections rise 650% year-over-year

Trojans have re-entered the enterprise cyber security spotlight as researchers at Malwarebytes report that trojan detection on corporate networks rose 200 percent between Q4 2018 and Q1 2019. The trend represents a shift away from personal users as targets.

Year-over-year, researchers found a 650 percent increase in endpoint detections of trojans on enterprise networks. Some malware variants, like the Hidden Bee cryptominer, find success in disguising themselves as run of the mill processes like svchost.exe or dllhost.exe to avoid detection.

Detections of trojans at enterprises rose 650% year-over-year.



360 Insight

The findings represent a massive increase in trojan detections. These types of cyber-attacks often masquerade as normal processes and in light of the latest trend, companies need to be sure that they're able to identify them before they're able to do real damage.

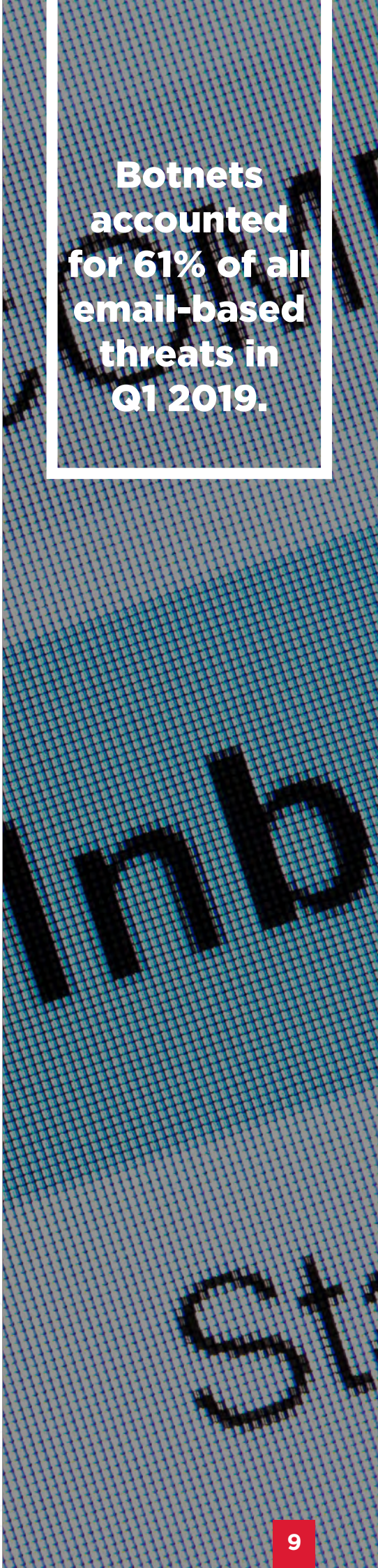
Enterprises should look to introduce next-generation antivirus and spam filters to better monitor their endpoints. With every single device that's connected to the network serving as a potential vehicle for the trojan, no stone can be left unturned.

Emotet botnet dominates email malware in Q1 2019

Researchers at Proofpoint found that Emotet was the most common email-based cyber threat that organisations faced over the course of Q1 2019. The botnet specialises in delivering malware disguised as attachments or links to seemingly legitimate websites.

Botnets accounted for 61 percent of all malware payloads that Proofpoint tracked in Q1 2019 and hackers used Emotet for virtually all of the cyber-attacks. Researchers reported that there's a substantial shift in payloads being delivered via links rather than attachments by Emotet as of late.

Botnets accounted for 61% of all email-based threats in Q1 2019.



360 Insight

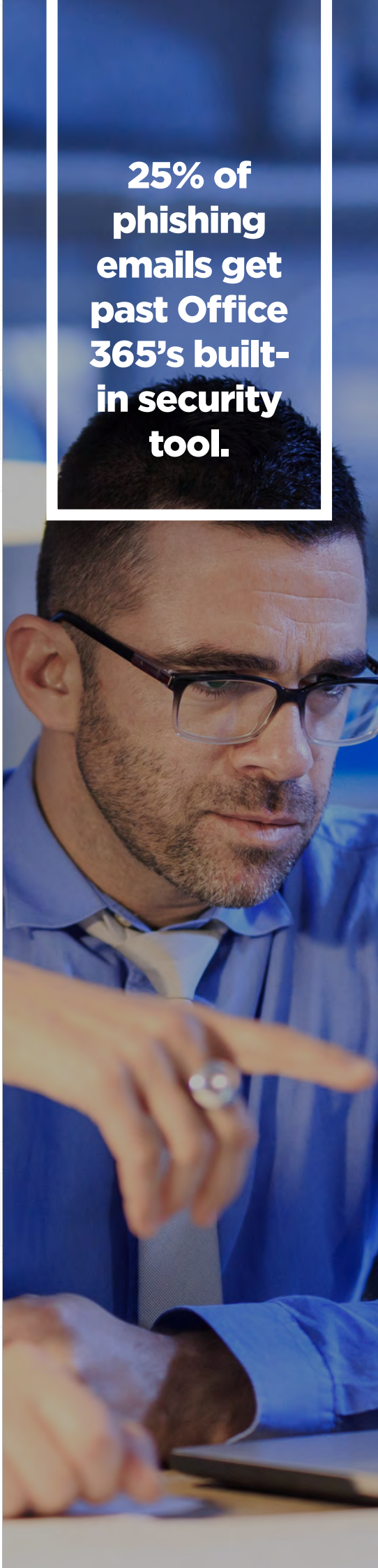
When nearly two-thirds of all email-based threats are using the same botnet, it's not just a coincidence. Emotet's influence as a reputable and effective botnet has grown since its creators shifted its role into a Hacking-as-a-Service model.

Email continues to be a high-profile and highly valuable target for cybercriminals. Spam filters are a bare minimum in any cyber security strategy and forward-thinking companies will look to adopt next-generation tools that can quickly react to massive international phishing campaigns.

Office 365 fails to stop 25% of phishing emails

Office 365's basic email security tool, Exchange Online Protection, was found to miss roughly one-quarter of all malicious phishing emails that were sent to its users. In total, over 560,000 malicious email attacks were discovered in the 55.5 million emails that were analysed in Avanan's Global Phish Report.

Common elements among malicious emails include links to WordPress websites as well as Bitcoin wallets. In spearphishing attacks, which made up less than 1 percent of email hacking campaigns, obfuscation was a common tactic.



360 Insight

Email remains the primary form of communication in corporate settings and hackers know that it's one of their best bets to infiltrate a network. Avanan's study shows that these bad emails are making their way through Office 365's anti-phishing tools. Next-generation email filtering and spam detection can go a long way towards preventing the next cyber-attack.

Companies should avoid using legacy protocols like IMAP in their email servers. A Proofpoint study found that IMAP was incredibly unsecure due to hackers' ability to potentially bypass MFA, and researchers found that it was the most commonly abused legacy email protocols.

Exposed data up 50 percent due to misconfigurations

The amount of exposed consumer and corporate data rose 50 percent over the previous year, researchers at Digital Shadows reported. The digital risk business found a year-over-year increase of roughly 750 million exposed files, with the total now sitting at 2.3 billion files.

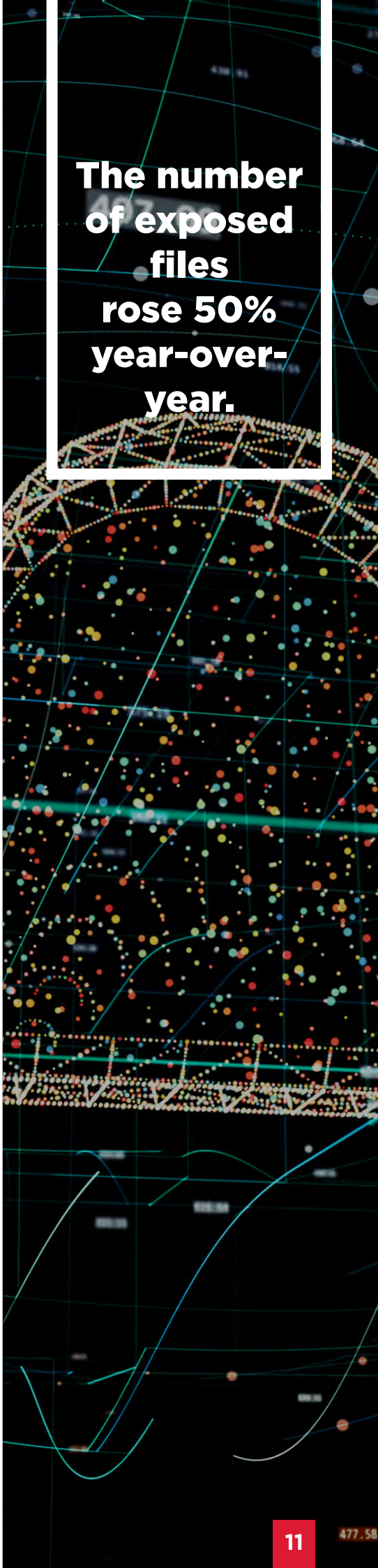
Researchers found that one-fifth of the top 1,000 Docker containers were vulnerable to a data leak, and that misconfiguration was to blame. Amazon S3 buckets and basic Office 365 setups, while secure by default, often have security features turned off as a part of development or troubleshooting and may never see them turned on again.

360 Insight

Given that GDPR has been up and running for over a year now, it's ironic that the increase in regulatory oversight has also coincided with a bump in sensitive data exposure. Breaches due to unsecure cloud databases are just as dangerous as connecting a computer to the network without any cyber security software installed or permissions set.

During Office 365 deployments, default security controls can be turned off and administrators may forget to turn them back on, making them easy to exploit. Companies should regularly review the policies and permissions in place for their cloud database if they want to remain proactive in stopping threats.

The number of exposed files rose 50% year-over-year.



Employees sharing sensitive information via email, IM

Organisations are having their efforts to contain sensitive data undermined by their workforces, according to a report from Igloo Software. Its 2019 State of the Digital Workforce study found that 60 percent of employees openly share sensitive files via email.

The rise in popularity of workplace messaging apps like Google's Hangouts or Slack's collaboration platform hasn't gone unnoticed. Nearly one-third of employees admit to sharing sensitive data on these platforms, regardless of whether they're approved as secure under the company's cyber security strategy.

360 Insight

Collaboration is changing quickly and security strategies may struggle to keep up with its pace. But failure to understand how files are being shared within the workforce can leave a company susceptible to damage from a third-party data breach, especially if vendors aren't vetted.

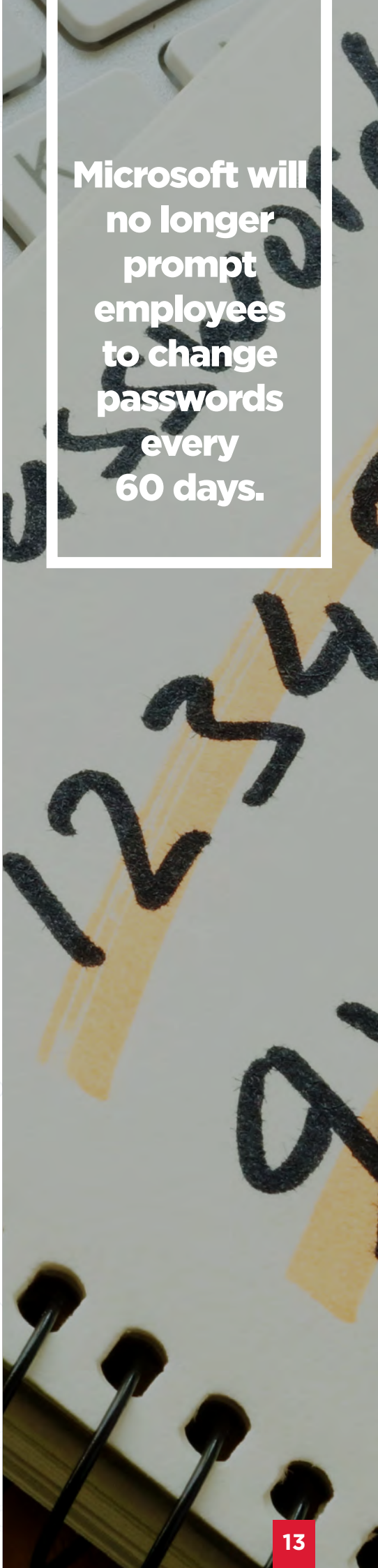
Regularly scheduled in-person cyber security training can help dissuade rogue employees from sharing sensitive data on potentially dangerous platforms. All approved forms of communication should be clearly whitelisted and strict permissions surrounding access to sensitive files should be in place.

Microsoft scraps its password reset policy

In its May 2019 update, Microsoft did away with its longstanding mandated enterprise password changes. The built-in security feature once reminded employees to set new passwords every 90 days, and most recently every 60 days.

The change comes on the back of a number of recent developments surrounding passwords and how to make them more effective. It was only two years ago that the organisation behind the NIST framework deemed mandatory password changes ineffective, as users often resort to weaker passwords in exchange.

Microsoft will no longer prompt employees to change passwords every 60 days.



360 Insight

Data breaches and leaks give hackers access to a trove of passwords that they can then use in automated password stuffing attempts. Given the recent innovations in AI, simply adding an extra symbol at the end of a password doesn't necessarily preclude hackers from guessing it.

Microsoft is likely doing away with password changes for two reasons: because they understand it causes more headaches than safety, and to pave the way for a more secure future using new tools and passwordless logins. By having strong, unique passwords for each account then it becomes easier to identify the source of data leaks – and shore them up – much easier.

FIDO2 certifications get Microsoft closer to passwordless world

Microsoft announced that its Windows Hello biometrics-based security system official received FIDO2 certification from the FIDO Alliance. After the May 2019 Windows 10 update, users will be able to switch to passwordless login for a variety of websites and apps.

The update will allow Mozilla Firefox users to replace their traditional passwords with the passwordless login for FIDO-enabled websites. Microsoft Edge and Google Chrome users will get the feature in a future update.

360 Insight

Account security is a hot topic issue given how unsecure the string of letters, numbers and symbols can be – and the far-reaching impact of a resulting security incident. Microsoft seems to be all in on biometric-based account security and getting FIDO2 certification was a big step for it.

The Fast ID Online (FIDO) Alliance is composed of a number of large technology companies, including Microsoft, and was created in an attempt to design a more secure future. The continued adoption of its certifications could mean that traditional passwords could be out the door over the next few years.

Spammers using Google Services to deliver campaigns

Kaspersky Lab researchers have found that spammers are taking advantage of Google's integrated ecosystem of services to delivery spam. Google Calendar, Google Photos, Google Forms, Google Drive and Google Analytics have all been leveraged in some way.

The spammers take advantage of the fact that people on Google can often communicate with anyone with few barriers. In the case of Google Calendar, spammers will set up an unsolicited meeting invite with the spam located in the details.

360 Insight

Spammers targeting Google Services represents another example of hackers exploiting the expanding attack surface presented by the interconnected world of apps. Within that emerging threat area, Google is no exception.

Companies must be cognisant of their varying degree of cyber defences (between internal and external systems) and build appropriate threat and risk management models to quantify exposure and detect possible abuses. The debate between user convenience and security is an age-old one and it's vital that companies are aware of the pay-offs that they're making.

Google reveals it stored passwords in plaintext

Google told a portion of its G Suite enterprise customers that their passwords were stored in its internal systems in plaintext. The security incident stemmed from a faulty process concerning its password setting and recovery functionality that the company implemented in 2005.

The issue reportedly affected a small number of its 5 million enterprise customers on G Suite. It was spotted by internal employees and fixed before any of the information was improperly accessed by internal employees or external threats.

A small number of G Suite enterprise customers had their passwords stored in plaintext.

360 Insight

Google isn't the only company to be found storing passwords in plaintext, with one German website receiving a fine under GDPR in 2018 for doing so. It has yet to be revealed whether Google will face any ramifications via GDPR.

The finding highlights the need for users to have a variety of passwords that they use for different accounts. If hackers were to get a password from G Suite that was then able to be used for tens of other accounts, they would be able to wreak havoc across an enterprise.

Thousands of websites compromised in supply-chain attack

Researchers discovered that formjackers had compromised at least seven different vendors, planting malicious code on thousands of websites in the process. Alpaca Forms, RYVIU, AppLixir and AdMaxim were among the third-party websites that hosted the malicious code.

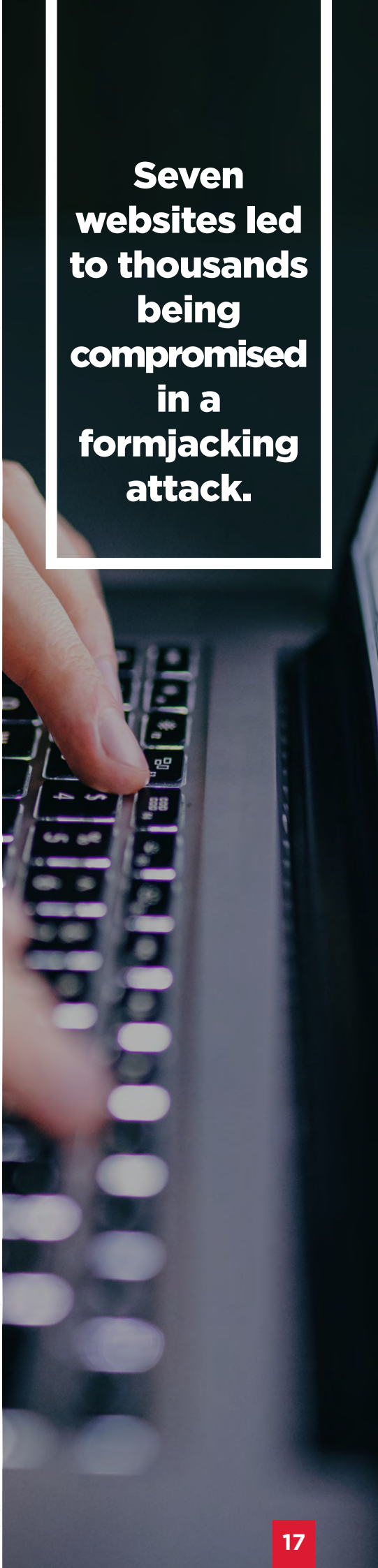
The breach allowed the suspected lone hacker to gather all data entered in forms on websites that used these third-party vendors. The stolen information, which included financial and other sensitive details, was then shipped to a server located in Panama.

360 Insight

Formjacking has grown into the cyber-attack du jour as of late, with MageCart recently featuring in a number of high profile campaigns on Forbes' magazine and Leicester City Football Club, among others. Attackers compromise third-party vendor websites as a means to infect the supply chain.

Many of these attacks take just a few extra lines of code to launch, making them increasingly difficult to spot. Companies need to regularly review their supply chain to ensure that third-party vendors are doing as much as possible to prevent cyber-attacks from taking place.

Seven websites led to thousands being compromised in a formjacking attack.



Intel reveals ZombieLoad vulnerability in modern chips

In a discovery reminiscent of Spectre and Meltdown, Intel revealed that a new vulnerability dubbed ZombieLoad could be used to extract data from a device. The vulnerability, which impacts all Intel chips created since 2011, is seen as both difficult to exploit and fix.

The vulnerability takes advantage of speculative execution, which is a function that's commonly used to improve chip speed. It's estimated that a fix to ZombieLoad could significantly reduce speeds, with some saying by as much as 40 percent.

The ZombieLoad vulnerability affects all Intel chips created since 2011.

360 Insight

If Spectre and Meltdown taught us anything, it's that hardware has more holes than you might think. ZombieLoad confirms it, giving the hacking community another method of extracting data from a device by bypassing many of the security solutions in place to stop just that.

ZombieLoad isn't the most efficient means of gathering sensitive data and it's more likely to return rubbish than gold. But it's another important development in the world of hardware security, where vulnerabilities can potentially be more devastating than their software counterparts.

Quarterly report spotlight: Verizon

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.

Verizon is well known in the cyber security community thanks to its tireless efforts in creating the Data Breach Investigations Report. Nothing changes in its 12th annual edition, which explores the tens of thousands of security incidents that took place in 2018.

In its 2019 Data Breach Investigations Report, Verizon breaks down a number of findings, including:

- Major cyber-attacks that took place in 2018
- Summary of findings
- Results and analysis
- Incident classification patterns and subsets
- Victim demographics and industry analysis
- Data breaches in:
  - Financial and insurance
  - Healthcare
  - Professional, technical and scientific services
  - Retail
- Year in review

You can read the entire **Verizon 2019 Data Breach Investigations report here.**

Verizon breaks down data breach statistics by industry for an in-depth analysis.

SIGN UP FOR OUR NEXT ISSUE

Want to receive the Cyber Security Risk Radar into your inbox each quarter?

Click here to sign up for our 'News & Insights' emails.

www.integrity360.com

Integrity360

your **security** in mind