CYBER SECURITY RISK RADAR

CONTENT

2 Executive summary

4 More cyber attacks in first half of 2020 than in all of 2019

5 Supply chain is the weak security link for 92 percent of US companies

6 QR codes lead to security concerns data shows

7 New Zealand's Exchange's massive DDoS attack: what went wrong?

8 CEOs could be held personally liable for cyber attacks that kill

9 Microsoft suggests a rapid transformation in cyber security

10 Shopify data breach illustrates the danger of insider threats

11 Morgan Stanley sued - with $5 million data breach suit

12 Drop everything and secure remote workforce, Gartner warns

13 SANS shares details on attack that led to data breach

14 Garmin outage caused by confirmed WastedLocker ransomware attack

15 Office 365 will let you manage phishing simulation emails

16 Report spotlight: Cost of a data breach

Integrity360
your security in mind

OCTOBER 2020

Q4

Executive summary

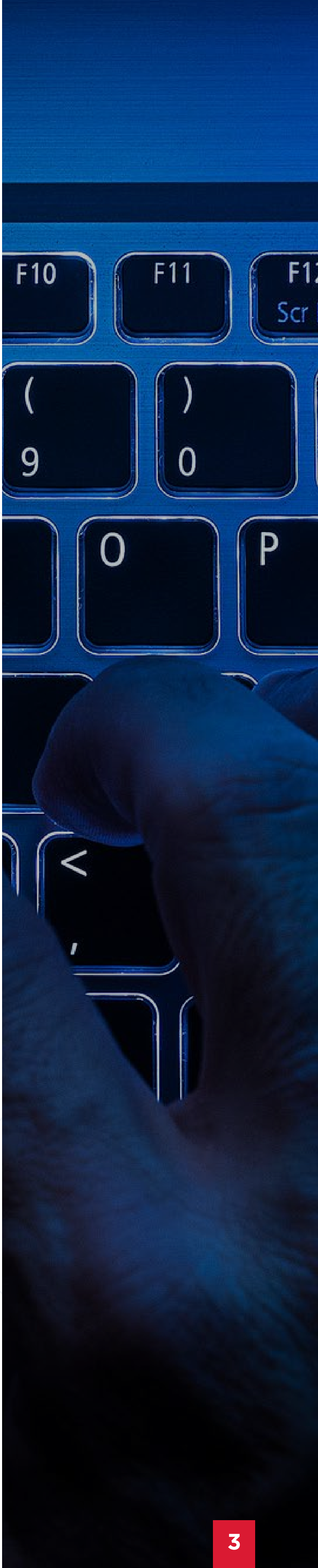
This quarter brings with it significant increases in the number of phishing, malware and cyber security attacks recorded. While the world has turned massively towards remote working in the wake of the pandemic, the security risks that come with that transformation are only just beginning to be understood.

This edition of the Risk Radar takes a deep dive into 12 of last quarter's most impactful cyber security stories. Furthermore, details are shared on lessons learned from these incidents.

- ✓ This year will go down in the history books for many reasons. One of those is the **massive increase in cyber attacks in the first half of 2020 than all of 2019.**
- ✓ **Supply chains have proven to be the most vulnerable part for organisations** in a recent study. 92% of firms are vulnerable at this point of their operations.
- ✓ QR codes are convenient and ideal marketing tools during Covid-19. **They're also channels for malware to be embedded and distributed.**
- ✓ A massive DDoS attack shut New Zealand's stock exchange.
- ✓ **Cyber attacks that result in death could see CEOs included in the culpability.**
- ✓ **Organisations are prioritising cyber security upgrades** as Covid-19 continues.

CONTENT MARKETING AWARDS
2019 BEST USE OF CONTENT CURATION

- **Insider threats need to be taken as seriously as external ones,** as the Shopify hack shows.
- **Morgan Stanley didn't follow best practice when discarding old computer equipment.** Now the bank is being sued for $5 million by more than 100 of their customers.
- Gartner has warned that the most pressing item on the to-do lists of firms should be **securing their remote workforce.**
- SANS has announced that they will share details of the data breach they've experienced with the cyber security community.
- **Garmin fell prey to a WastedLocker attack** and had to temporarily close some of its services.
- **Office 365 is releasing functionality to help organisations train and educate their staff on phishing attacks.**



More cyber attacks in first half of 2020 than in all of 2019

Crowdstrike has recently released a study that shows cyber attacks were higher in the first six months of 2020 than during the whole previous year. In fact, hands-on-keyboard malicious attacks were 154% higher than in 2019 for the same time period. While there are many reasons for this spike in attacks, the mass migration to working from home due to Covid-19 has played a massive role in the increase.

Not all industries were targeted equally by cyber criminals. Financial, technology and telecommunications organisations have been targeted most heavily during 2020. However, an increase in cyber attacks on manufacturing companies has also been noted.

360 Insight

The Crowdstrike report also showed a big increase in malware-free attacks, which now outnumber malware attacks. Crowdstrike defines malware-free attacks as ‘those in which the initial tactic did not result in a file or file fragment being written to disk.’ This data point reinforces the need for effective Endpoint Detection and Response (EDR) and anti-virus solutions that don’t rely solely on signatures.

Record number of cyber attacks in 2020

Supply chain is the weak security link for 92 percent of US companies

The old adage that a chain is only as strong as its weakest link is ringing true for supply chains. The Target breach in the USA in 2013, which was so severe the U.S. Justice Department became involved, has proven to be one of many rather than the exception to the rule. BlueVoyant has recently shared research that indicates 92% of U.S. organisations have suffered data breaches because of their supply chain in the last year.

Many of the companies included in the survey come from the financial services, utilities and energy, business services, health care, pharmaceutical and manufacturing. Another alarming statistic in the report was how 69% of the companies affected by data breaches had no idea what security measures their supply chains have in place.

360 Insight

One of the most effective countermeasures to supply chain threats is a robust Privileged Access Management solution (PAM). Privilege escalation attacks occur outside of the supply chain, but in the supply chain, it’s harder to detect when an unknown third party is trying to get access. A Privileged Access Management solution enables supply chain managers to define and enforce privileged account access controls across the supply chain.

Supply chains can be the weakest link

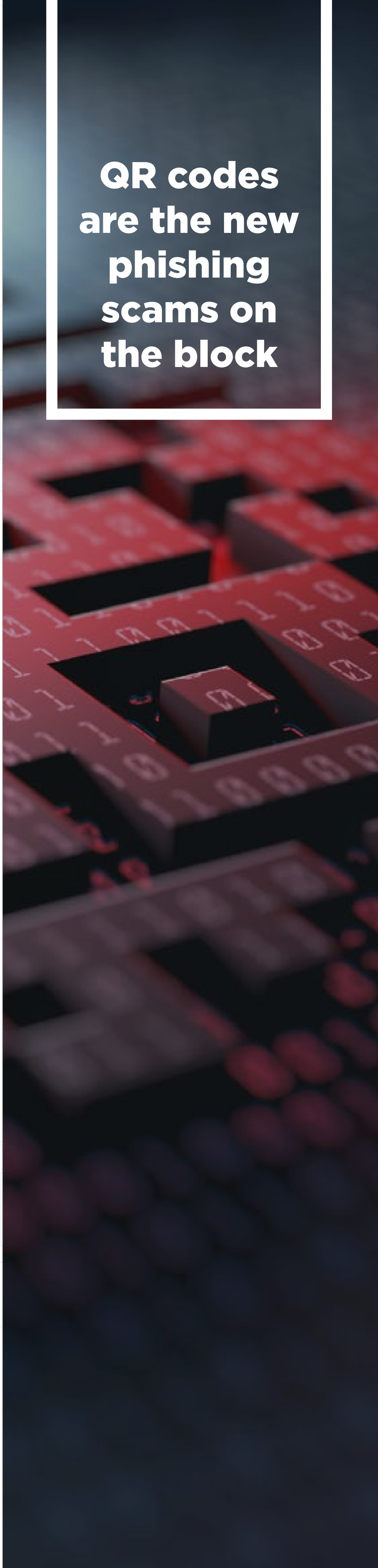
QR codes lead to security concerns data shows

The use of Quick Response (QR) codes is soaring during the pandemic. Businesses are using this technology to stay in touch with customers and promote their goods and services as an alternative to paper brochures. However, QR codes are open to a lot of malicious activity without people realising the inherent risks.

A recent survey, run by MobileIron, highlights how 71% of respondents said they couldn't "distinguish between a legitimate and malicious QR code". An example of a QR attack is a cyber criminal embedding a dangerous URL or custom malware in a QR code that can lift data from a mobile device. Businesses are urged to apply stringent security strategies to their mobile marketing campaigns.

360 Insight

Traditional endpoint protection solutions struggle to identify the latest malware injection vectors, like QR scanning. Investing in effective endpoint protection that can detect and isolate malware processes not only reduces risk but avoids onboarding technical debt.



QR codes are the new phishing scams on the block

New Zealand's Exchange's massive DDoS attack: What went wrong?

The NZX, New Zealand's stock exchange, has fallen victim to an extortion attempt in the guise of a huge distributed denial-of-service (DDoS) attack. The attack happened in August.

Fortunately, the trading engine of the NZX was not affected. However, the stock exchange still had to shut down due to its website being under attack and all public announcements being paused.

The NZX struggled for days with its service provider to secure more robust DDoS mitigation services. Only once these were in place did the website resume online.

360 Insight

Availability is often overlooked in the CIA triad. Keeping mission-critical resources available to users from any location over any device is the standard for most organisations. Resilient business architecture is the best defense against massive DDOS attacks. Business processes and their interdependencies should be reviewed regularly, preferably using an independent trusted third party.

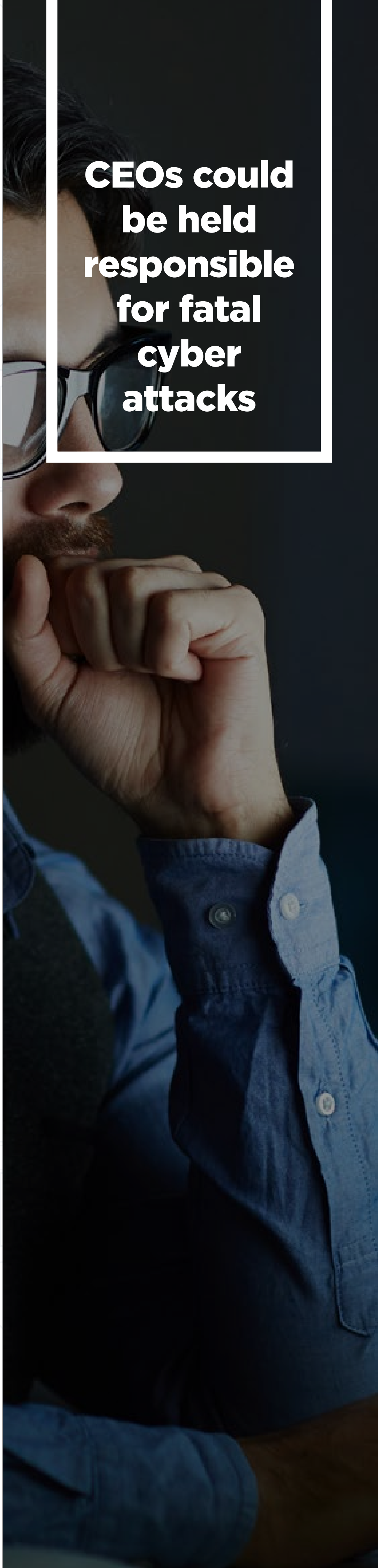
DDoS shuts NZX stock exchange

CEOs could be held personally liable for cyber attacks that kill

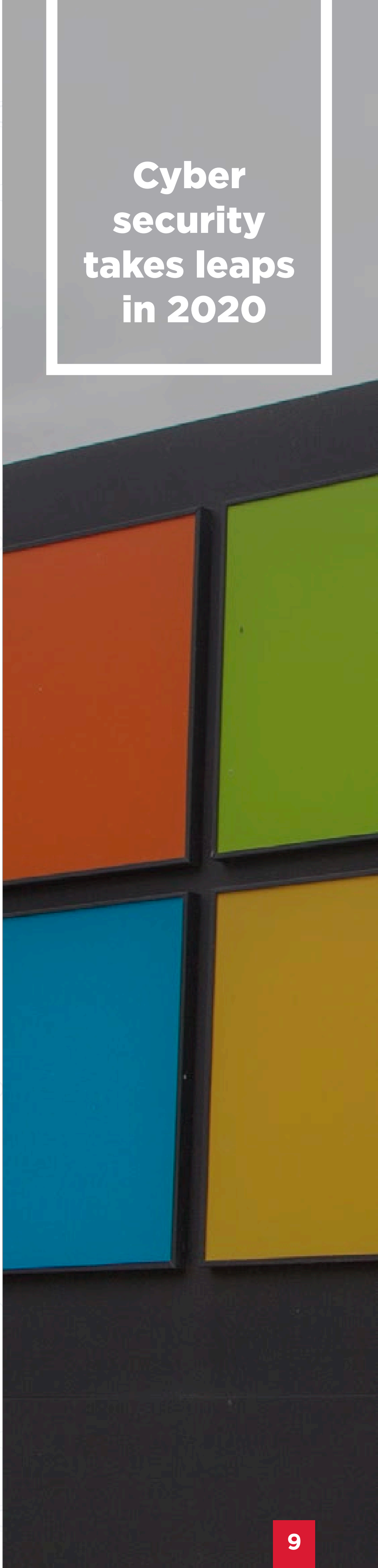
Who is ultimately responsible if a cyberattack ends up killing someone? According to Gartner research, by 2024 the person, or people in the firing line, will be CEOs and leadership teams. CEOs will no longer be able to hide behind corporate legal teams if cybercriminal activity ends in fatalities on their watch. These dire consequences are set to be actioned sooner rather than later as IT systems, operational and Internet of Things devices converge.

360 Insight

The consequences of an OT breach can be dire; from halting production to the worst-case scenario where people are killed. Yet, investment in securing Operational Technology is minimal because it increases the cost of production. Holding executives accountable for OT breaches may be a step forward in increasing commitment to and investment in OT Security.



CEOs could be held responsible for fatal cyber attacks



Cyber security takes leaps in 2020

Microsoft suggests a rapid transformation in cyber security

While no one is thinking in terms of silver linings with the ongoing Coronavirus, there’s a growing recognition that the pandemic has jolted organisations into taking their cyber security strategies more seriously. It’s an often repeated phrase now that in the first two months of the pandemic, the world went through “two years’ worth of digital transformation”.

Microsoft recently released a report that examined companies of 500 employees and more in the USA, UK, India and Germany. The report specifically investigated how the pandemic threat has impacted on long-term cyber security, budget, staffing and how companies have updated their security.

360 Insight

The network perimeter has been eroding slowly over the past decade at a pace that organisations could handle, however the COVID-19 pandemic has caused an enormous and sudden shift that has caught many off-guard. You must assume your perimeter is breached and embrace a Zero-Trust Security mindset.

Shopify data breach illustrates the danger of insider threats

Data breaches don't just come from external cybercriminal threats. Increasingly, merchants and businesses are having to pay extra attention to the threat of insider danger.

This trend has most recently been highlighted by a data breach at Shopify that affects close to 200 retail partners. Alarmingly, the breach did not happen due to a "technical vulnerability", but from two employees in the support team who maliciously used personal data. Tesla has also recently disclosed a "malicious insider" incident.

360 Insight

Insider threats account for approximately one third of an organisations risk. This rule of thumb has stayed remarkably consistent in the annual Verizon Breach Report over the years. There are excellent resources and methodologies available to further refine the risk for specific organisations. The level of risk for insider threat is specific to the organisation. The starting point for mitigating this risk should be an independent assessment from a trusted security partner.

Cyber attacks can originate close to home

Morgan Stanley sued - with $5 million data breach suit

A customer of Morgan Stanley is bringing a $5 million class action lawsuit against the investment bank. The reason for the lawsuit is due to the bank's failure to protect customer information when the company discarded obsolete computer equipment.

The case is being tried in the U.S. District Court in the Southern District of New York on behalf of 100 customers, all affected by the data breach. The lawsuit relates to two incidents, in 2016 and 2019, when Morgan Stanley discarded old computers and computer equipment.

360 Insight

Organisations that handle sensitive data must have a policy for Data Encryption and for Data Destruction. Ensure you use secure encryption for the data you need to store, and when you no longer need that data ensure the destruction of it securely.

Investment bank on the block for $5 million lawsuit

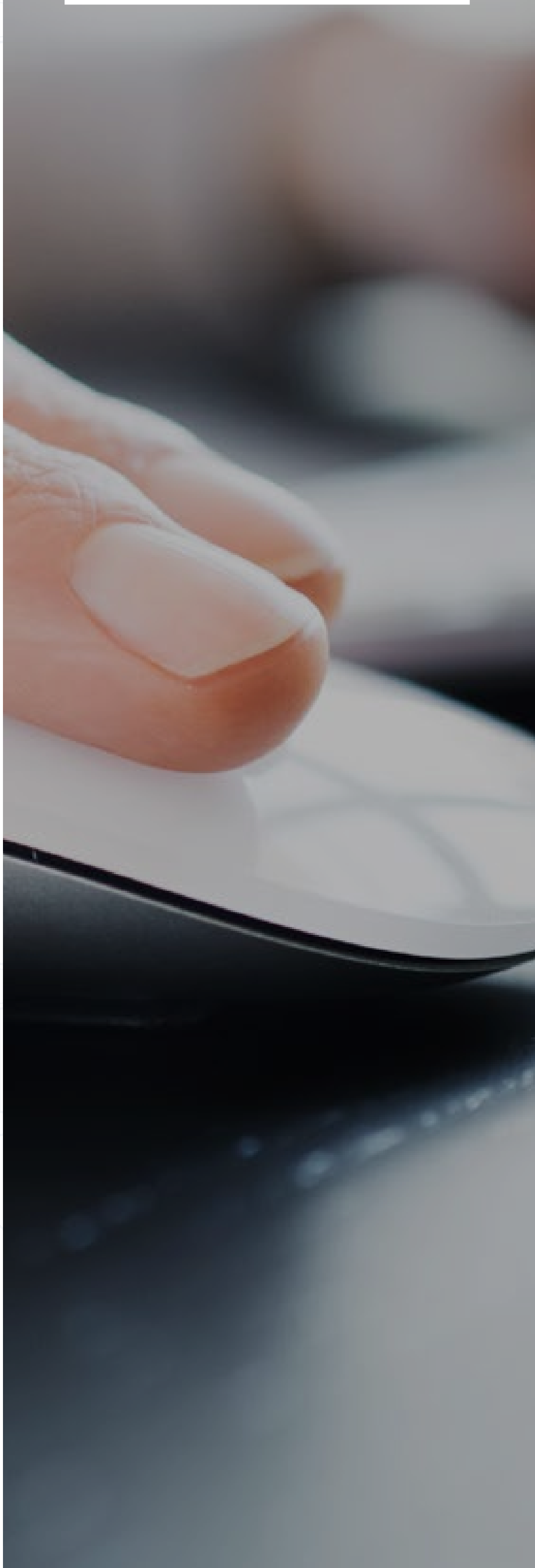
Drop everything and secure remote workforce, Gartner warns

Gartner has recently warned, at the Gartner Security & Risk Management Summit 2020, that all cyber security strategies have to start with strengthening the security around their remote workforces.

While it's acknowledged that organisations will have many security priorities, the Covid-19 pandemic has upended all of them and radically changed how people work. The flexibility and continuity of remote working has also opened up security risks for firms.

360 Insight

Delivering cloud based technical controls has never been so important with the users now geographically distributed. Organisations should look first to web, email and cloud based proxies, CASB and the evolving SASE models for solutions.



Securing remote teams has to be #1 cyber security strategy

SANS shares details on attack that led to data breach

In mid August, SANS announced that they had experienced a data breach. An employee had fallen for a phishing scam that led to more than 500 emails being sent on to attackers.

Included in the emails were an estimated 28,000 records of personal information data for SANS members.

SANS has also shared that they will be releasing the details of the attack, once their own reviews are complete, to help the cyber security community.

360 Insight

Incident Response and eForensics are often not prioritised in an organisation's budgets. The specialist skills required for reliable eForensics drives some of this behaviour. Both capabilities can be dramatically improved with the use of specialist partners who can provide timely expert resources on a retainer basis. This can improve response time and protect brand equity in the event of a breach. SANS timely, transparent and confident response is a good example of the value of investing in Incident Response and eForensics.

28,000 personal records compromised in data breach

Garmin outage caused by confirmed WastedLocker ransomware attack

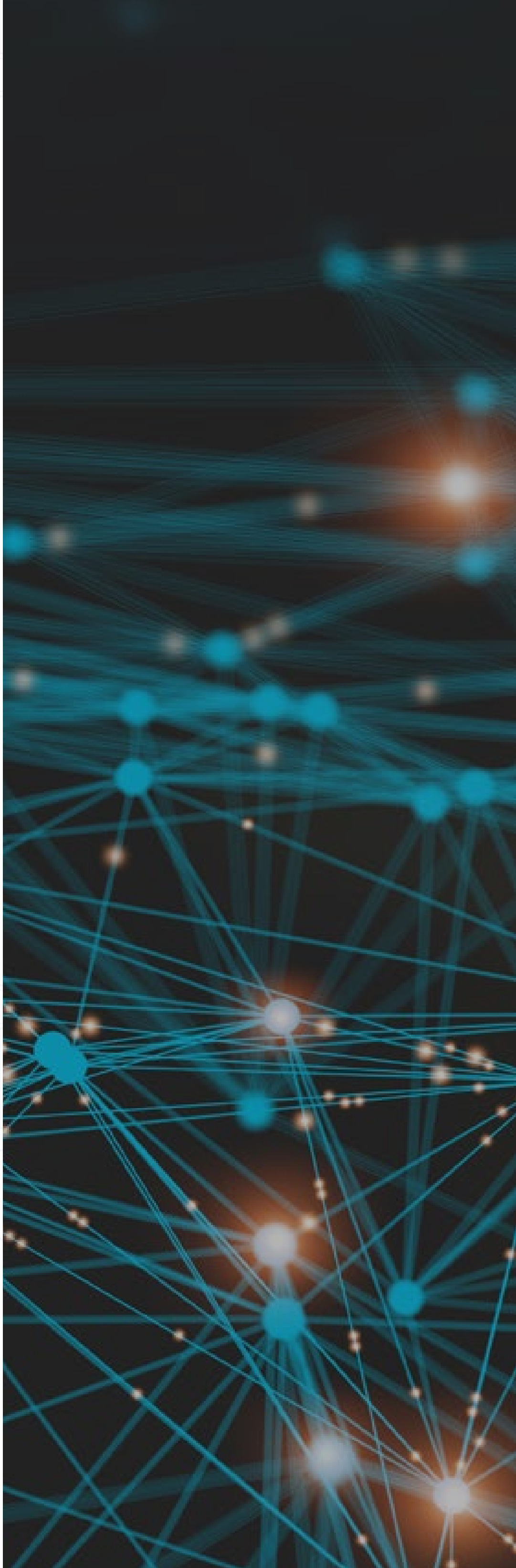
In early July, Garmin, the wearable device maker, paused some of its services and shut down its call centres after what was initially termed a “worldwide outage”. It’s now known that the “outage” was in fact a WastedLocker ransomware attack.

It was Garmin’s branch in India that first sounded the alarm for the attack, and highlighted the reduced performance of Garmin Express, Garmin Connect mobile and the website.

360 Insight

Ransomware is becoming commodified with Ransomware as a Service RaaS platforms now lowering the barrier to entry for sophisticated malware attacks. EDR, Deception Technologies and Browser Isolation Sandboxing are just three preventative controls that should be considered in conjunction with a well-planned Incident Response capability.

Garmin falls prey to WastedLocker ransomware attack

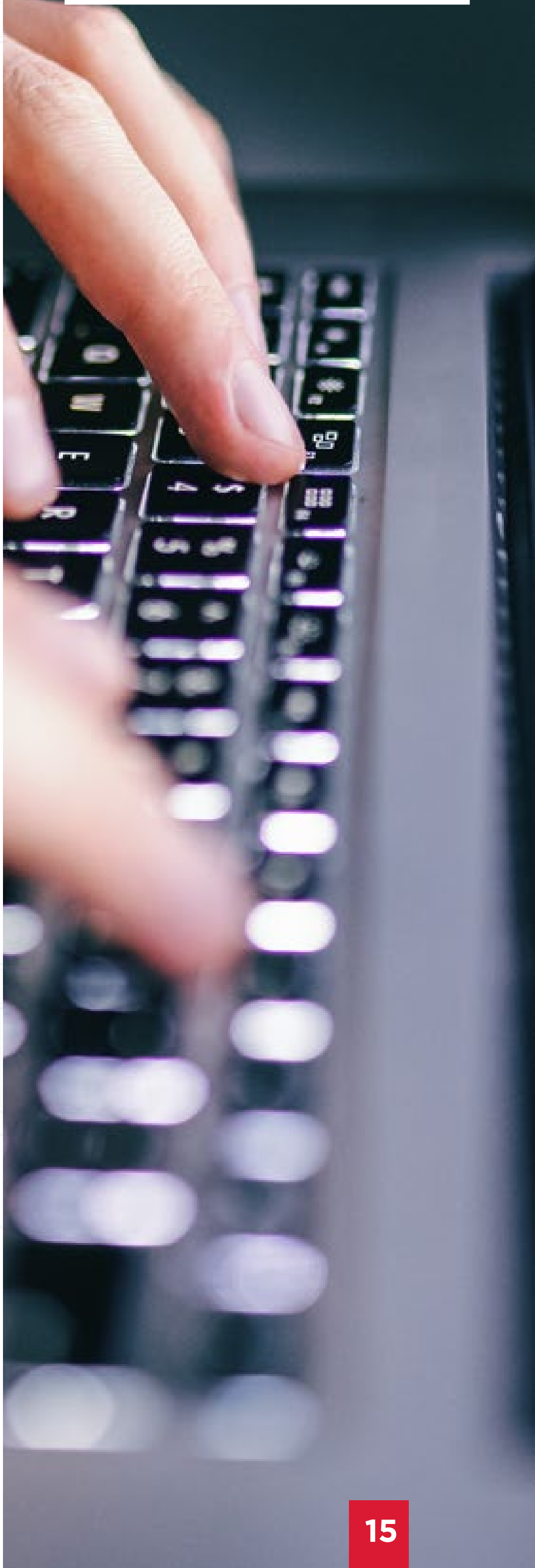


Office 365 will let you manage phishing simulation emails

Educating workforces about phishing scams occasionally requires sharing emails with malicious URLS or attachments with employees. Microsoft is adding a support feature that will allow organisations to do this through a self-remediation portal on the Office 365 platform.

Microsoft has released information that showcases the feature and says on the roadmap page, “we understand that from time to time, customers may want to ensure delivery of certain messages containing malicious content for specific reasons, such as phishing simulations and training”.

Microsoft provides functionality for phishing training emails



360 Insight

A phishing simulation campaign that’s not convincing to users can be a costly and distracting exercise. It will be interesting to see how effective this new feature is compared to best in class phishing simulation solutions like KnowBe4.

Report spotlight: Cost of a data breach

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.

The Ponemon Institute's 2020 Cost of a Data Breach study has become a household name in an industry brimming with reports and information. The insights provide a baseline for the research surrounding data breaches and their effect on businesses and the threat intelligence community at large.

In the 15th annual edition, Ponemon explores in-depth a variety of factors surrounding data breaches, including:

- ✓ Global findings and highlights
- ✓ Root causes of a data breach
- ✓ Factors that influence the cost of a data breach
- ✓ Security automation trends and effectiveness
- ✓ Time to identify and contain a data breach
- ✓ Longtail costs of a data breach
- ✓ Potential impacts of Covid-19
- ✓ Cost of a mega breach
- ✓ Steps to help minimise financial and brand impacts of a data breach

You can read the entire Ponemon 2020 Cost of a Data Breach study here.

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

UK OFFICE
90 Long Acre, Covent Garden
London, WC2E 9RZ
+44 2033 973 414

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

You Tube

Integrity360
your **security** in mind