SECURITY CHALLENGES 2020

A Bytes Market Report

BYTES Smarter together

Check Point SOFTWARE TECHNOLOGIES LTD.

About this Market Report

At the start of lockdown IT teams everywhere had to enable home-working at a pace and scale never seen before. Projects that would normally take months to plan, design, test and deploy were having to be completed in days.

"Microsoft has seen two years' worth of digital transformation in just two months." Satya Nadella, CEO Microsoft, April 2020.

Quick decisions had to be taken and normal due process and diligence had to be relaxed. However, the period of grace has now passed. Organisations are now having to take stock of where they are, retrospectively plugging security holes and updating employees on the increased cyber risks they need to help mitigate.

Consequently, security priorities have shifted and are today focused on what could be argued are the fundamentals in securing this new way of working, such as implementing security measures to protect Office 365 and client Endpoints.

However, with so much to do and so little time to do it, there is a real risk that some IT security teams are making assumptions about their environment that are questionable, such as the over confidence and misunderstanding that having a Mobile Device Management solution in place serves as an effective security solution, which it does not.

Another example of over confidence is in the capability of their employees to spot a malicious phishing attack.

On average respondents to our survey were 71% confident their people were competent in this area. However the reality in most cases is far from this as phishing attacks have risen hundredfold since March and there has been very little time to deploy mass training refreshers and new infrastructure.

Given the race to secure and plug the holes left by the mass mobilisation of home workers, IT security teams need help understanding where they should be focusing their resources. To help provide this guidance, we surveyed 198 UK IT Professionals ranging from IT Managers, CISOs, and Heads of IT from a variety of organisations.

This Report provides their views on what is critical to IT security success in 2020 and includes further insights and commentary from David Rawle, Group Chief Technology Officer at Bytes, and Ian Porteous, Regional Director, Security Engineering, UK&I at Check Point.

Report Summary

What is clear from the findings detailed in this Report is the lack of consistent security confidence that exists across IT security teams. Security Analysts that are confident in one area, are less confident in another. There are also key security areas which have risen in importance in the last 6 months which remain under-resourced and of primary concern. No-one seems confident in every element of their businesses security, and even when people appear to be confident, they give different answers to the same question.

This confusion and contradiction are almost certainly due to the rapid speed that new "home-working" systems have had to be deployed. The normal planning, design, testing, documentation, checks and balances that would ordinarily take place have had to make way for rapid business transformation, creating lack of certainty, recording and monitoring of the security precautions and solutions that have been deployed. It's been a case of enablement first, and security second.

We expect this to change as time progresses and running this same survey in 6 months time would potentially give very different results.

As well as a lack of consistent confidence in security, the survey has surfaced some interesting themes:

1. **Securing Office 365 remains a top priority.** With more employees using and relying on Office 365 as their primary productivity suite they are populating it with more and more data. Protecting this new data from an abundance of new and evermore sophisticated threats is now reaching a critical phase.
2. **Endpoints remain vulnerable.** With cyber attackers turning their attention to trying to attack the VPN by exploiting home-working vulnerabilities, it has never been more important to ensure endpoints are fully protected and regularly patched.
3. **Employees are not as cyber-savvy as they need to be.** With phishing attacks continuing to develop in their sophistication and with cyber criminals now targeting mobile phones alongside client computing devices, it is essential all employees receive up to date and relevant cyber essentials training on an on-going basis.
4. **MDM is not mobile security.** The findings suggest most organisations feel their mobile devices are secure. However in most cases, this cannot be assumed. Whilst most have an MDM solution, these do not provide any level of meaningful security and may provide a false sense of security which leaves organisations unnecessarily exposed.
5. **Data deemed "Most important" is at risk.** Most respondents (57%) feel they either don't have the sufficient security technology or don't have technology that is configured properly to protect their most important data, exposing them to potential material fines and/or reputational damage.
6. **There are too many vendors to manage.** Nearly half of respondents feel their security environment is too complex and costly, due to them having to manage too many security vendors. This is negatively impacting their ability to maintain the required skills needed to configure and manage the various security products.

Survey Results

In light of COVID-19, how would you rank the following areas of concern (1= highest and 6= least)?

	1	2	3	4	5	6
Datacenter	17.62%	7.77%	16.58%	15.03%	19.69%	23.32%
Cloud (compute)	8.81%	21.24%	15.03%	11.92%	23.83%	19.17%
Cloud (productivity and collaboration)	30.57%	17.10%	18.65%	17.10%	10.88%	5.70%
Mobile	12.95%	19.17%	20.73%	23.83%	11.40%	11.92%
Endpoint	21.76%	20.21%	16.06%	15.03%	16.58%	10.36%
DLP	8.29%	14.51%	12.95%	17.10%	17.62%	29.53%

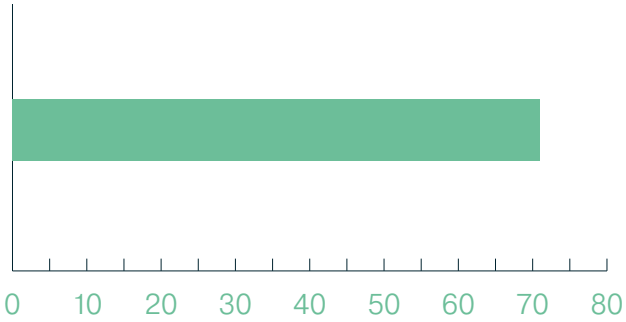
Clearly the two front runners here are Cloud (productivity and collaboration) and Endpoint, which given the mass mobilisation of home workers is to be expected. What needs to be appreciated is that most "new" home workers do not have a company-supplied computer so are having to make do with using (and sharing) the family device. Such a setup is very challenging for IT teams, particularly with regards to providing secure connectivity, application availability and data integrity. This is BYOD in its rawest form. IT teams should be commended on enabling home workers so quickly, but now recognise they need to address some of the short-cuts they had to take to get people working remotely.

What is less expected in the survey findings is that **DLP is deemed the lowest priority, despite Endpoint being one of the highest**. An effective DLP strategy will help solve the Endpoint concern so should be high up the priority list.

Now that workers are enabled, the focus needs to shift from enabling and protecting workers in doing their daily roles to understanding what data is where and gaining visibility that none is leaving the organisation, being manipulated or worse exfiltrated – so not just focus on protecting the device or cloud environment itself, but understand what is happening within it. With less than 10% of people making this their priority right now, we would urge businesses to look there next in an effort to avoid data risk.

Neil Smith, Head of IT Operations at Spark Energy comments, "Ensure cloud and on-prem are both covered, ideally in the same solution to provide better simplicity/governance."

The number of malicious phishing emails has increased by over 667% since March. From a PEOPLE perspective (ie employee awareness/training), how confident are you that you are protected from such cyber threats?



This score is the average rating across all respondents.

The findings from this question show that on average, people are **71% confident their employees are sufficiently trained to be able to spot malicious emails.** This is highly unlikely to be the case and may be creating a false sense of security, particularly when you consider most organisations are not properly testing their employees to this effect, and if they are, are they continuing to do so?

With fewer employees working in supervised, firewall-protected environments, where they know actions are monitored, and with more people working flexibly from home where their own guards will be down, it has never been more important to ensure employees are cyber-savvy.

Attackers are taking advantage of this as they are aware businesses have had very little time to roll out effective cyber awareness training programmes and deploy new infrastructure. The number of cleverly designed and targeted phishing campaigns has risen sharply.

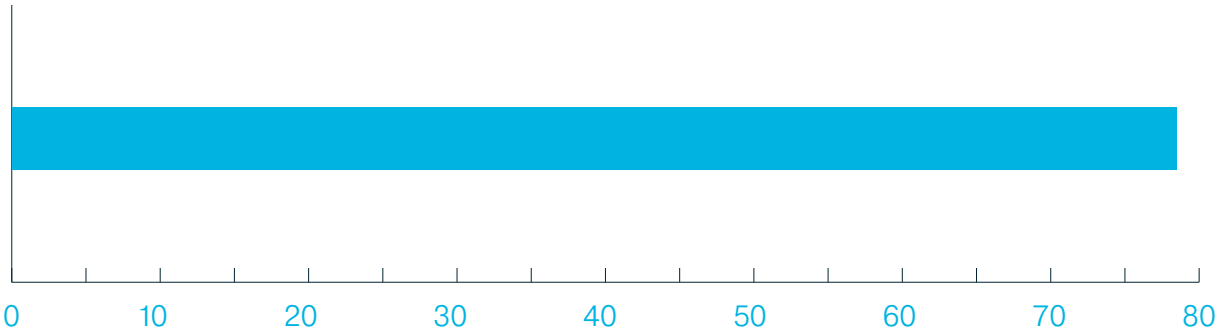
Even if a 71% confidence score were accurate, is that enough as it still leaves a big margin for error? You only need to look at some of the very high-profile attacks that have taken place, such as the Twitter Spear phishing attack, to recognise there is still a lot of do with regards cyber awareness education.

The other blind spot many organisations are yet to address is to do with mobile phones as these are a growing target vector for cyber attackers. Even if the findings are taken at face value, nearly 1/3 of respondents are not confident their employees are cyber-aware. As such, we would advise caution and suggest a review into this area.

Given the explosion of COVID-related and home-worked-related phishing emails, and the increase in malicious newly registered "covid" and "zoom" related domains, many of which are sophisticated in their design and serve as effective data-collection landing zones, it is no wonder employees are being caught off guard and underpins the need to have an on-going strategy around cyber essentials training.

This is a view shared by John Oliver, IT System Services Manager, from Newcastle Building Society, "Don't forget to educate staff/people through regular training."

Same question but from a TECHNOLOGY perspective - what's your confidence in your phishing-attack prevention?



This score is the average rating across all respondents.

A confidence level of 78/100 is perhaps a little high but is there or thereabouts. What this does show us is very few businesses have confidence levels up in the 90s – and in this era of lack of visibility and rising threats there are clear technology gaps which can be addressed (more on those later) which can help businesses move that confidence and security up to the level that their business would demand.

It is also advisable, given the speed in rollout of a myriad of new platforms to support connectivity in recent months, to dedicate time now that the initial wave has passed to undertake due diligence to make sure any technology in place does indeed have the required capability to detect and prevent such attacks. This would avoid a mismatch between reality and perceived security levels.

From a security perspective, how confident are you the following areas are secure and fit for purpose?

	HIGHLY UNCONFIDENT	NOT THAT CONFIDENT	CONFIDENT	HIGHLY CONFIDENT
Endpoints	2.59%	15.03%	61.66%	20.73%
Mobile phones	2.60%	27.08%	55.21%	15.10%
Secure Remote Working	2.59%	11.40%	59.07%	26.94%
Identity Access Management	2.59%	20.73%	56.48%	20.21%

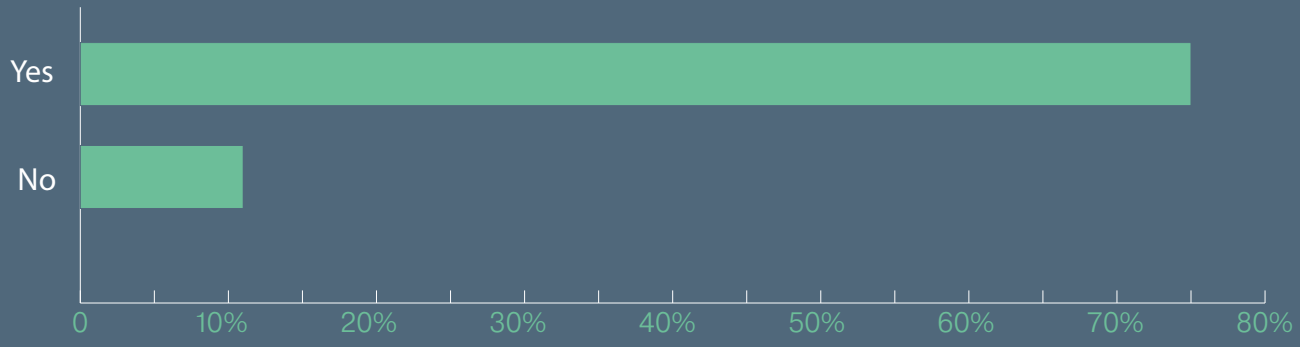
The two areas that raise concern here are Endpoints and Mobile Phones. Starting with the latter, there is a wide misconception within most organisations that having a Mobile Device Management (MDM) solution in place serves as a security solution. Just to be clear - it doesn't.

MDM provides an effective means of managing remote devices but offers very little in isolation with regards to security. Given mobile phones are an increasingly used attack vector, attention should be paid to the security on them, particularly given the increased malware success-rate associated with mobiles. It only takes a well-crafted and malicious SMS from the "IT department" asking the recipient to update their password, or click on a file as proof they have read the latest home-working policy, and the attackers are in.

Mobile devices are not yet treated or secured as 'computers/endpoints' in their own right as such yet, which may be a real mistake due to prevalence of use, their access to corporate resources and the misconception that MDM = Mobile Security.

The other area of concern is Endpoint protection, as only 20% of respondents are highly confident they have a solution that is fit for purpose. With an abundance of home workers, criminals are successfully breaching less-protected endpoints and attacking the VPN so it **is highly recommended organisations conduct an audit of what endpoint security solutions they have in place, how they are configured, and what level of protection they deliver to the organisation, to avoid any security risks.**

Do you put any security on your company mobile phones?



A False Sense of (Mobile) Security

In line with the commentary above, due to the misunderstanding of the level of security protection Mobile Device Management solutions provide, it is highly unlikely 75% of respondents have a sufficient security solution in place that offers meaningful protection for mobile phones, creating a false sense of security.

Furthermore, Cisco's Security Intelligence and Research Group (TALOS) recently reported a malicious campaign that leveraged an MDM solution to control victim's devices, compromising a corporate-owned MDM and spreading malware to more than 75% of the corporate's devices via the compromised MDM.

This incident underscores the importance of distinguishing between managing and securing mobile devices. Managing a mobile device means installing applications, configuring settings, and applying policies on multiple devices at once. Securing a mobile device means protecting it from malware threats and attacks.

Businesses should be ensuring that they have both (distinct) bases covered, especially in today's mobile working era.

MDM's most prominent feature, arguably the reason for its existence, is also its Achilles' heel – a single, central control for the entire mobile network. If that platform is breached, so is the entire mobile network.

With the recent exponential rise of BYOD, managing and securing them has become a whole lot harder as many MDM solutions do not cover them. As such, if protecting mobile phones is deemed important, it is recommended a review of the current solution is undertaken.

David Rawle, Group Chief Technology Officer at Bytes said, "Without continuous device-health monitoring in place, organisations are blindly trusting that its mobile fleet will remain unimpacted by threats. This blind trust is particularly dangerous in the current environment where employees are permitted to use their personal devices for work, load personal apps onto a work device, and/or use the internet for personal web browsing."

In relation to the security of the data residing in Cloud Applications, how concerned are you about the following:

	NOT CONCERNED AT ALL	NOT THAT CONCERNED	CONCERNED	HIGHLY CONCERNED
Your Office 365 environment	19.79%	53.65%	23.96%	2.60%
Your virtual Conference environment	21.24%	52.85%	22.80%	3.11%
Other permitted Cloud Apps (eg, Dropbox, Box, Slack)	19.27%	32.29%	33.85%	14.58%
Shadow IT	7.81%	33.85%	38.02%	20.31%

Interesting findings from this question. For starters there is a contradiction with the findings of question one. In question one, 47% of respondents stated they were not concerned about DLP, yet in this question nearly 58% state they are either concerned or highly concerned about Shadow IT, which is a key source of data risk.

It suggests that where apps are not provided/ sanctioned by IT there are naturally higher concerns due to lack of visibility of the app itself and user behaviour. The average organisation has hundreds of apps in circulation and many IT teams do not see a high proportion of them so attempts to control untested and unknown applications whilst not limiting productivity is key.

The true extent of data leakage and theft possibilities from Virtual Conference platforms remains underestimated.

Nearly 75% of respondents stated they are either "not that concerned" or "not concerned at all" about their virtual conference environment, and yet sensitive data including links and documents can be shared freely and often without thought via these platforms using functionality such as Chat.

It appears therefore that investment is needed in data loss awareness training to help counter this growing concern. Just because an application is provided by or Sanctioned by IT does not mean that users are not using it in ways which pose a risk to data and company, which may be being underestimated or overshadowed by the fear of Shadow IT risk.

Finally, over 25% of respondents state they are either concerned or highly concerned with their Office 365 environment.

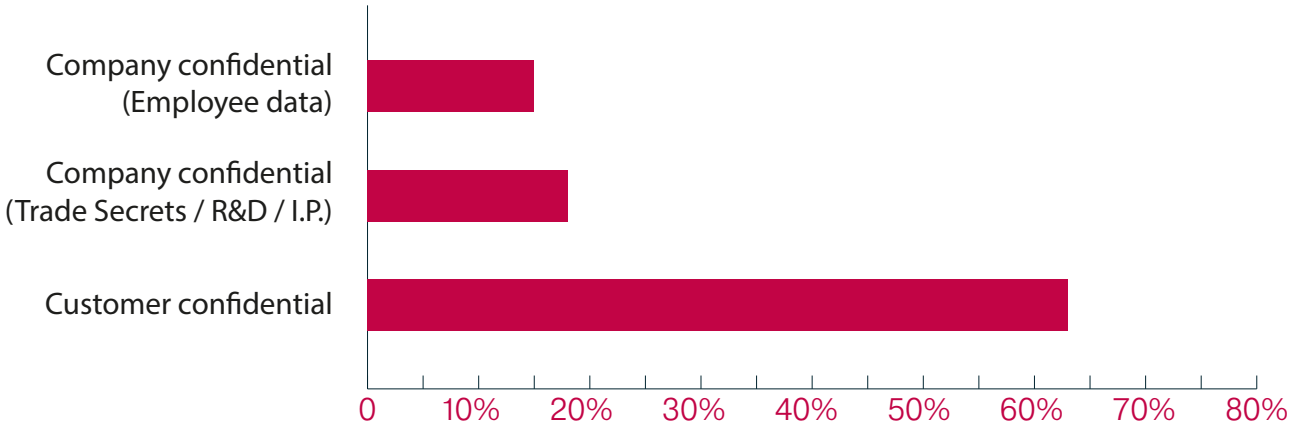
This is most likely due to the increased use of Office 365 since the pandemic broke and the amount of data being shared within it.

If there are concerns with Office 365, one of the most deployed, oldest and "tried and tested" cloud applications, there is need to layer security on top of ANY application as the responsibility for security sits internally with IT and not the cloud provider.

These findings are despite the fact that in an earlier question, 85% of respondents stated that were either "confident" or "highly confident" in their secure remote working measures. A similar confidence score was given to having fit-for-purpose endpoint security. It seems clear that when we get into detail and scratch the surface of security confidence, there are still gaps and concerns even for the most confident of respondents.

Having such contradictions highlights the complex challenges associated with best-practice security management and the misunderstandings that exist around some of the technologies available.

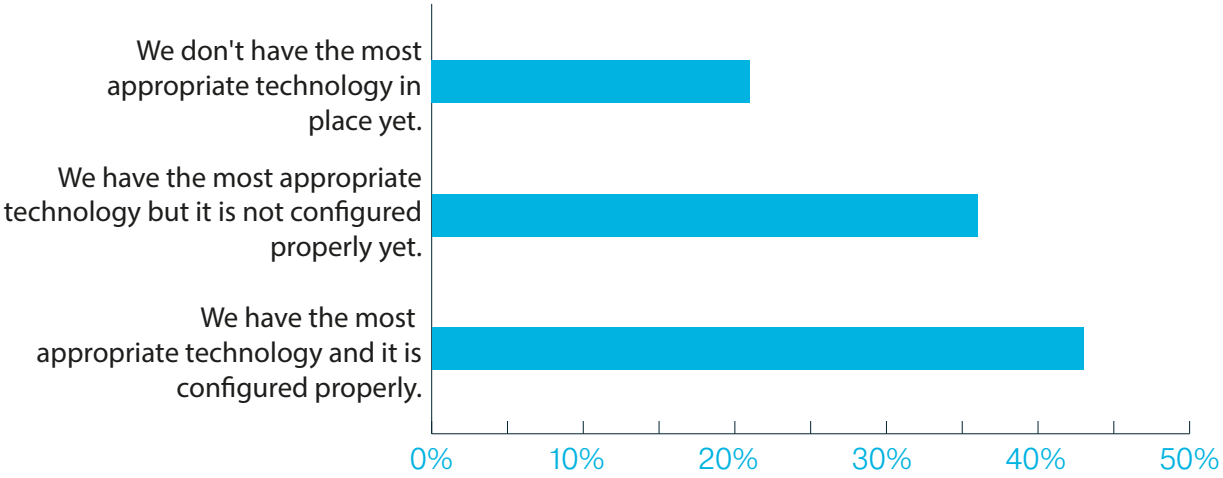
Which data will be most damaging to you if it were lost?



There is no surprise in these findings, particularly given the introduction of the GDPR and the associated punitive fines that organisations risk incurring should a breach occur.

There is also increased recognition of the significant reputational damage that breaches can cause with this data type and the cost and time needed to rebuild trust when customer data is at stake.

With regards to having appropriate technology in place to protect your most important data, which of the following statements is most applicable to you?



The findings of this question raise an alarm, and once again are in contradiction to some of the earlier findings in this Report.

43% of respondents to this question state they have the most appropriate technology and that it is configured properly, and yet earlier on respondents stated they were 78% confident in their security technology. This suggests people may not be as confident about their security solution as previously stated.

Misconfigurations are a growing issue

However, perhaps more alarming is that 20% of respondents state that they don't have the right technology to protect their most critical data, their crown jewels, that's more than one in five organisations. 57% of respondents state they either dont have the right technology in the first place to protect their most important data or they have the right technology but not configured correctly. This latter point is a growing area of risk for organisations. Indeed, Gartner recently stated that "through 2022, at least 95 percent of cloud security failures will be the customer's fault," and that "through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws."

These findings suggest many organisations are never going to benefit from the investments they are making in their security stack and what's more, many may think they have the right protective measures in place, but due to their misconfiguration they don't, thereby creating a false sense of security.

Working with external specialist security providers, such as Bytes, will help ensure the right systems are in place and that they are configured correctly.

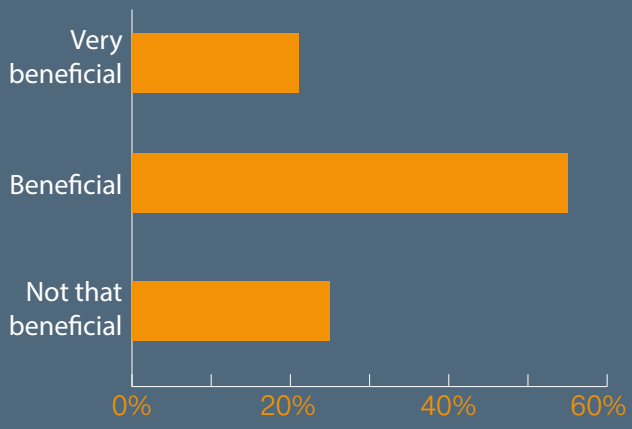
Simon Lindsay, IT Security Manager at Total Gas & Power, comments, "The basics are more important than ever. If you haven't got assets and vulnerabilities visible and under control everything else is a waste of time and money."

In relation to your security set up, what are your 3 main pain points?

Whether it was from a technical or administration perspective, nearly half of the respondents to this question stated “Too many vendors” as being a pain point. This would explain many of the other findings as trying to manage multiple vendors is always going to put a strain on upskilling employees and lead to escalating costs. Lack of appropriately skilled security analysts may be a key contributor to the misconfiguration commentary in the previous question and poses a material risk to organisations.

A better, less risky and more sustainable approach is to have fewer vendors with common controls and configuration options, that way skills can be leveraged across multiple products, and better commercial deals can be negotiated.

How beneficial would it be if you could pay a single price (per user per month/year) for a solution that covered the majority of your security needs?



No real surprise in these findings, particularly given the universal need for organisations to be as agile as possible and reap the cash benefits associated with paying for products and services monthly rather than via cash-hungry CAPEX arrangements. The Check Point Infinity solution is a great option in these situations. Check Point Infinity is the first and only architecture designed to deliver the most complete real-time threat prevention against Gen V cyber-attacks and leverages Check Point's most advanced products and technologies across all networks, cloud, endpoint and mobile – all managed by a single, consolidated console. Bytes is an Award-winning Check Point Elite Partner and have the necessary expertise to provide the relevant advice and insights in this regard.

Simon Fanthorpe, IT Director of Alpha Real Capital comments, "Reduce complexity by using a smaller number of key systems with the coverage you need, ensure you have a single place to look at all security alerts and settings."

BYTES Smarter together

Key Takeaways

David Rawle,
Group Chief Technology Officer at Bytes

“It is clear that this is a report generated by organisations in transition who might not have yet seen all of the impacts of remote working.

The material increase in phishing attacks is evidence of this with over 70% of respondents reporting they are confident in their people and technology to prevent this issue. However the experience of Bytes is in contradiction to this as even in the absolute top performing organisations, 20% of employees will and do open phishing emails.

If you combine this statistic with the fact that there has been a 667% increase in phishing emails since lockdown started in March, organisations are currently highly exposed. Only by covering every vector, including mobile phones, can organisations even begin to win the battle to secure their data.”

1. More focus needs to be placed on securing Office 365.

With more data residing in Office 365 than ever before, it is becoming increasingly more business critical so needs the right level of focus and investment to ensure it is properly secured and patched on a regular basis, together with a greater focus on what is happening to the data within Office 365, eg. where it is moving to and who is accessing it.

2. All endpoints, including mobile phones, need enhanced security measures.

Cyber criminals are successfully breaching endpoints and attacking VPNs. They are also implementing highly targeted SMS campaigns with a disproportionally high degree of success. The solution to this problem is part technical and part employee educational. Both aspects need a continuous review and improvement strategy to ensure they remain effective.

3. The majority of organisations are putting their critical data at risk.

The wrong technology and misconfiguration of the right technology is leaving critical data unnecessarily exposed to unauthorised and unwanted access. According to Gartner, "through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws. Misconfiguration is therefore is a growing cause of successful cyber attacks so organisations are advised to work with organisations that can help them mitigate against this avoidable risk.

4. Trying to manage too many vendors is leading to gross inefficiencies and exposure to unnecessary risk.

Security is a complex business but can be made less complex by working with fewer vendors. A shortage of skills is the biggest issue facing the security industry and organisations that are trying to manage multiple vendors just exacerbates this. Reducing the number of vendors will help ensure security analysts remain skilled and able to properly configure and maintain all necessary security systems. It will also help reduce costs.

5. Confidence is not as high as it needs to be.

The rapid mass mobilisation of home workers has left security professionals feeling a little numb and lacking in confidence. To help overcome this, organisations are advised to solicit the services of an expert security partner, such as Bytes, who can help undertake a full security audit and put together a security readiness roadmap.

Future Trends

Cloud

We expect to see threat actors continuing to target specific company departments and employees in order to reap more lucrative rewards. The growing popularity of public cloud environments has led to an increase of cyber-attacks targeting resources and sensitive data residing within these platforms. While more organisations move to the cloud, awareness that they are still responsible for the security of data held there is still lagging.

Practices such as misconfiguration and poor management of cloud resources will remain the most prominent threat to the cloud ecosystem.

Network

We expect to see an increase in DNS Attacks. DNS Attacks target one of the most important mechanisms that govern the internet – the Domain Name System (DNS). The DNS oversees resolving domain names into their corresponding IP addresses and it is a crucial part of the internet's trust chain.

Such attacks target DNS providers, name registrars, and local DNS servers belonging to the targeted organisation and are based on the manipulation of DNS records.

DNS takeovers can compromise the whole network and enable multiple attack vectors: control of email communications, redirection of victims to a phishing site, and more. One of the biggest advantages DNS attacks provide is the option to issue legitimate looking certificates by Certificate Authorities which rely on DNS to verify that you are the legitimate holder of the domain in question.

IoT

For enterprises IoT devices will remain the weakest link in security and we predict that more attacks will make use of them as their point of entry as well as being targets in and of themselves.

This is due to them being harder to secure while being adopted into the corporate infrastructure at an increasing rate, thereby enlarging the attack surface.

A recent industry study reveals: 67% of enterprises have experienced an IoT security incident.

From smart TV's, IP cameras, and smart lifts, to hospital infusion pumps and industrial PLC controllers, IoT and OT (Operational Technology) devices are inherently vulnerable and easy to hack. Many of these devices come with out-of-the-box security flaws such as weak or hardcoded passwords, misconfigurations in the operating system, and known vulnerabilities (CVEs). Their inherent security weaknesses and the fact that they are poorly protected made IoT devices an attractive target for attackers.

Hackers are continually looking for ways to exploit device vulnerabilities so they can attack the devices themselves or better use them as an entry point to the corporate network. IP cameras can be used to spy on users, medical devices can be shut down, and critical infrastructure (such as power grid controllers) can be taken over to generate colossal damage. The risk is high and enterprises across different industries are exposed.

Consolidation

Due to the skills shortage across the security industry, and the need for a single pane of glass across lots of emerging technologies, we are expecting to see organisations consolidate the number of security vendors in their environment to a smaller and more manageable number.

No longer will organisations automatically aim to address emerging threats with new technologies from new vendors, but instead will be turning to their existing suppliers, such as Bytes, and asking how their current vendor stack can be used to mitigate such threats.

Compiled by Ian Porteous, Regional Director, Security Engineering, UK&I at Check Point.

Need advice with your Security Strategy?

There are three ways Bytes can help you

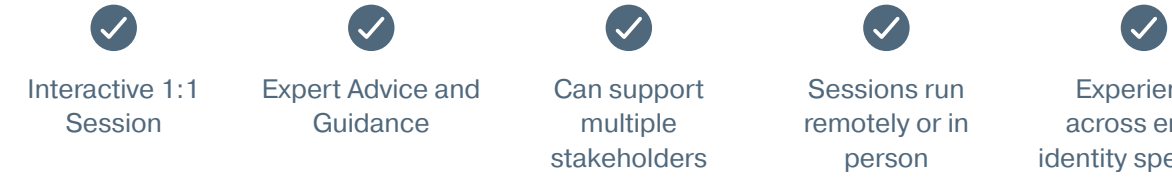
1. Vendor Consolidation Assessment and Roadmap

A great place to start on your journey to understanding the unique benefit that your business can gain from consolidating security is to start with a free Bytes Security Consolidation Workshop.

Our expert engineers work with you to identify your key security challenges, then walk you through the various options that you have to strengthen your security posture whilst consolidating and simplifying your security stack. The result – a clear map of your journey to consolidated, efficient security supporting:

Our quality process:

What you can expect:



2. Office 365 Threat Assessment and Roadmap

One of the key concerns raised by organisations in this report was a lack of perceived confidence and control in Microsoft Office 365.

Bytes are in a unique position to assist businesses in securing their Office 365 environments due to our strong partnerships with both Microsoft and leading complementary security partners such as Check Point.

Gain peace of mind and see all Office 365 security threats with a free Office 365 Security Healthcheck from Bytes and Check Point.

For 30 days you will gain complete visibility of

Current threats in your Office 365
from both known & unknown malware

Your Level of Protection
The strength of your organisation Office 365 security

Emerging Unknown Threats
Your exposure to spear-phishing, ransomware and more

Remediation Recommendations
How Check Point technology can plug security gaps found

Simple Setup - No Cost

This non intrusive detection-only Healthcheck can take as little as 30 minutes to set up after which you will benefit from Check Point's award-winning Cloudguard SaaS solutions to protect your Office 365 for 30 days at no cost, gaining a true picture of the security health of your Office 365 environment and detecting advanced threats for an entire month, for free.

In the first week one UK Professional Services organisation found

Ø 126 Malware Events

Ø 2006 Phishing Events

Ø 680 Shadow IT Events or Unsanctioned Applications

What will you discover? Find out - Request your Healthcheck today.

3. Correct Configuration Assessment and Roadmap

Making sure you avoid misconfigurations and breaches

Bytes free Cloud Security Snapshot provides complete visibility of your public cloud assets and their compliance across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform or all three combined.

A clear, detailed and complete security map of your cloud architecture – with results within an hour – at no cost.

Our Cloud Security Snapshot, powered by Check Point's award-winning CloudGuard Dome9 cloud compliance solution, detects and plugs your cloud security and compliance gaps - for free, so you can

- Assess Security Posture
- Detect Misconfigurations
- Model and Enforce Best Practice
- Protect against Identity Theft
- Prevent Cloud Data Loss

A true picture of your cloud assets & compliance across multiple public clouds

Cloud Assets Configuration
Identify which applications and workloads you have running on the cloud.

Public Exposure Levels
Understand the applications and workloads that are public-facing and more vulnerable to threats.

Network Topology
Review your network layout and understand areas prone to threat exposure.

Security Groups
Discover and classify your security groups by varying exposure levels.

Traffic and User Activity
Review how applications and workloads interact and the traffic associated.

Simple Setup - No Cost

In as little as an hour after set up you will be detecting and plugging your cloud security and compliance gaps across multiple public clouds, **for free**.

Explore how Check Point's advanced technology can detect & plug gaps in your cloud security and governance with our free no-obligation 30 day Cloud Security Snapshot.

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £500m, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Check Point

Check Point Software Technologies is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks.

Check Point offers multilevel security architecture, “Infinity” Total Protection with Gen V advanced threat prevention, which defends enterprises’ cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system.

With over 3,500 security experts, a world-acclaimed research and intelligence unit, and the broadest ecosystem of business and technology partners, Check Point protect over 100,000 organisations of all sizes across all industry verticals in over 88 countries across the globe giving them better digital experiences in a safer digital world.

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

To understand how Bytes can help you develop and enhance your Security Strategy, get in touch and start a conversation today.

BYTES | Smarter together

UK Head Office

Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

T 01372 418 500
E tellmemore@bytes.co.uk
W www.bytes.co.uk