Cybersecurity Predictions For 2020 And Beyond:

How Can SMBs Prepare For A Changing Cybersecurity Landscape?

October 2019

The State of Cyberattacks Now

Cybercrime is on the rise, but widespread underreporting hides the true figures

Businesses face potential cyber threats from all angles

What Does The Future Of Cybersecurity Look Like?

Businesses will become more proactive

Cybersecurity spending is set to increase

There will be a greater focus on the human element

UK cybersecurity post-Brexit

5G and IoT

Artificial Intelligence (AI)

Cybersecurity and the law

How Can Businesses Future-Proof Their Cybersecurity Measures?

The role of the cybersecurity team

What can businesses do to protect themselves?

What are the authorities doing about it?

Conclusion

Prevention is better than cure

Standing still is no longer an option

Cybersecurity Predictions For 2020 And Beyond: How Can SMBs Prepare For A Changing Cybersecurity Landscape?

As more of our personal and professional lives move to the online sphere, the risk of a cyberattack has become increasingly likely. The general understanding across the industry is that cyberattacks are commonplace now, both in terms of the frequency and scale of cyberattacks:

- Approximately half of all property crime is now online
- According to a YouGov poll, a business is nine times more likely to be a victim of cybercrime than burglary
- More than 60% of firms reported an attack in the last year, up from 45% the previous year
- Since the start of 2019, UK businesses face a cyberattack at a rate of once every minute
- 25% of medium firms and 20% of large firms report a cyberattack at least once a week

In the current forward-facing landscape, what can businesses do to ensure they aren't left behind, or worse, become the next cyberattack victim? This whitepaper will explore the current cybersecurity landscape, experts' predictions for the next few years, and ways businesses can future-proof their cybersecurity measures to prepare for the challenges ahead.

The State Of Cyberattacks Now

Cybercrime is on the rise, but widespread underreporting hides the true figures

Professor Vasilis Katos, Head of Computing at Bournemouth University says there is clear evidence of this in the figures gathered by cybersecurity experts – the amount of attacks witnessed in the last 5 years is greater than all preceding years.

Cybercrime does not discriminate. Larger companies are still the most likely targets, but surveys indicate that small and medium-sized businesses are becoming equally vulnerable. Hiscox's 'Cyber Readiness Report' found that more small firms faced cyber threats this year, with an increase from 33% to 47%. Meanwhile, medium-sized firms saw a huge jump in reported cyberattacks from 36% to 63% this year.

However, calculating the most accurate cyberattack figures is made harder by widespread underreporting. According to ISACA, 75% of people believe that the actual number of cyberattacks has been deliberately underreported, despite obligatory or legal requirements to do so. So why might the actual number of cyberattacks be higher than reported?

- **Businesses are worried about the consequences** – Reporting a cyberattack draws the attention of the public eye to the incident and having to deal with the repercussions, such as reputational damage, handing out financial compensation or paying fines. However, this is a common misunderstanding and reporting a cyberattack to the police is unlikely to lead to bad press.
- **"What's the point?"** – Identifying cybercriminals is notoriously difficult, and it is unlikely that a business will recover any lost data or finances, so many businesses feel apathetic when it comes to reporting the incident. Similarly, the time and expense involved in reporting a cyberattack often deters businesses from investigating, especially when those resources could be spent on recovery instead.

Businesses face potential cyber threats from all angles

These days, the cyber threat landscape is so dynamic that it can be hard to keep track of the all the ways a business can be attacked. These are the most common types of cyber threats any business could face:

Overall, the most successful attacks start with phishing emails. A 2019 government cyber security survey found that 80% of businesses experienced attacks from phishing emails, and an Oxford research paper drew similar conclusions – 72% of successful cyberattacks were related to fraudulent emails.

Of course, it is hard to overlook the impact of NotPetya and WannaCry. In 2017, these two ransomware attacks affected almost 250,000 computers across 150 different countries, including energy firms, major food production chains, as well the UK's National Health Service. It is estimated that the attacks cost over $10 billion and $8 billion respectively in damages, making NotPetya and WannaCry the most expensive cyberattacks to date.

What Does The Future Of Cybersecurity Look Like?

Businesses will become more proactive

These days, the risk of being attacked or hacked is not a question of 'if', but 'when'. While some businesses still have their heads in the sand, fortunately, cybersecurity awareness is on the rise and the risk of a cyber threat is quickly rising to the forefront of the agenda.

The latest Cyber Security Survey finds that 78% of businesses say cyber security is a high priority for their organisation's senior management, with around 40% within this figure saying that it is a very high priority for them. Samuel Leach, Director of Samuel & Co Trading echoes the sentiment of many businesses who already have a well-rehearsed cybersecurity strategy:

> "Having effective incident response capabilities that are tested regularly is key and enables organisations to respond quickly in order to mitigate the threat and identify the cause."

Therefore, it's no surprise that in the 12 months since a cyberattack, 78% of businesses have taken action to identify potential cyber risks. This is partly due to legal obligations such as GDPR compliance, but overall this is a positive upward trend. Davey Winder, Senior Contributor at Forbes says that for a growing number of businesses "an incident response plan is not an optional luxury - it's a cyber-essential."

Cybersecurity spending is set to increase

The average spend on cybersecurity is now $1.45 million, and the rate of spending is likely to accelerate in the coming years – two thirds of respondents were planning to increase their budgets by 5% or more. While larger firms tend to spend more on cybersecurity, we can also see a marked increase in investment across certain sectors such as Finance, Healthcare, and Information/Communications.

Jamal Ahmed, Privacy Consultant at Kazient argues that this growth could also lead to an increased demand for outsourcing cybersecurity and data protection solutions, if businesses are looking to bolster their cybersecurity but might not necessarily have the time or resources to develop a proper strategy.

However, smaller businesses shouldn't worry about the size of their cybersecurity budgets – the key is to think strategically and focus on your unique business priorities instead. Samuel Leach has some reassuring advice:

> "No matter how much you spend on cybersecurity, you can never do 'everything'. Even the world's largest banks, investment funds, and insurance providers have to prioritise their security resources to protect against the most likely (and most damaging) forms of cyberattacks."

There will be a greater focus on the human element

A cyberattack may just seem like lines of code, but humans are the ones who can make or break a business' cybersecurity defences. The general consensus is that hackers and cybercriminals are the most likely perpetrators of a cyberattack. However, a security breach can just as easily occur from within an organisation. A recent YouGov poll revealed that when it comes to cybersecurity risks, "48% of managers are more concerned about employees breaching data security than about cyber attacks from outside."

Edward Whittingham is Managing Director at The Defence Works, a cybersecurity training company that focuses on building employee awareness:

> "There has been an over reliance on technical IT measures for a long time and a huge onus placed up IT teams that it's their responsibility to prevent cyber-crime. Cybersecurity is everyone's

> responsibility and businesses should help address the human element [by] placing a real focus on developing a positive security culture throughout their organisation."

We can expect to see an increased demand for training that focuses on the human element – this has the potential to cover everything from war games for board members, to phishing email simulations for the average employee.

UK Cybersecurity post-Brexit

The UK remains a big player in the global cybersecurity landscape, but the political uncertainty that has come following Brexit is not without consequence. Professor Vasilis Katos says:

> "The UK cybersecurity industry must be well prepared with a clear plan on how intelligence sharing will be delivered post-Brexit in order to maintain their brand and trust."

There are a whole host of topics that could be discussed in further detail, but Davey Winder breaks down some issues businesses should keep an eye on in the future:

- Employment and skills gap – the UK is already suffering from a "major shortage of skilled practitioners [within] a widening threat landscape". Leaving the EU is likely to drive talent out of the UK market, as cybersecurity experts look to find better work elsewhere.
- GDPR – while GDPR is already part of UK law, when it is eventually updated there is a chance for discrepancies to arise between the UK and EU editions. This also creates the possibility of legal gaps where businesses may try and take shortcuts, and cybercriminals might exploit them.
- Information sharing – UK law enforcement is making efforts to collaborate with EU authorities, but this will be more difficult to achieve post-Brexit. On a larger scale, it has the potential to affect the workings of the Five Eyes Group, where the UK plays a key role.

Ciaran Martin, head of the National Cyber Security Centre has suggested that Brexit 'will not impact' UK-EU relations when it comes to cybersecurity. However, Dr Tim Stevens argues that Brexit could actually prompt businesses to re-evaluate and revise their cybersecurity strategy within an international framework.

The best way to properly assess the impact of Brexit on cybersecurity will be to consider both the short and long-term changes that will occur. But, we can predict that businesses will need to stay on their toes and react accordingly, whether the consequences are for better or for worse.

5G and IoT

The introduction of 5G and the Internet of Things (IoT) means all of our devices will be connected in an increasingly complex network. This includes your company computers, laptops, tablets, phones and voice-controlled assistants, and maybe even your personal devices too. While it certainly has its benefits, Holly Andrews, Managing Director at KIS Finance argues that this could allow hackers to infiltrate your entire network:

> "The main threat is that if one of your devices is hacked, that means they all are, and data can be stolen from any of them. Once this happens, the task of re-securing all of these devices is far greater than just having to deal with one entrance point or one employee."

This is where the UK's position in the global cybersecurity landscape will be especially important. Professor Vasilis Katos argues that international laws such as the EU Cybersecurity Act will protect member states for

now, but as mentioned before, any discrepancies in future editions may be amplified with the introduction of 5G and IoT.

Artificial Intelligence (AI)

Artificial intelligence is currently experiencing a period of huge growth and businesses are using AI to detect malware, verify users and improve cybersecurity in a number of ways. However, hackers are using AI to make cyberattacks faster and more efficient, as well as synthesise new forms of cyberattacks. One example of this is audio and video manipulation, also known as 'deepfakes'.

Deepfakes use machine learning to manipulate footage, falsely making it look like a person said or did something when they did not. While the technology is impressive, researchers have raised concerns over deepfakes and its potential uses in fraud, targeted hacks and cybercrime.

In March 2019, hackers used AI-based voice software to impersonate the chief executive of a British energy company, deceiving his managing director into transferring over $240,000 (£197,368) into a secret account. The software imitated the real CEO's voice so accurately and convincingly, that the subordinate complied even though he thought the request was 'strange'.

AI cyberattacks and the era of 'fake news' can erode trust, but this is also a good opportunity for businesses to sharpen their media literacy. We need to recognise that not everything is trustworthy, but that doesn't mean *nothing* is trustworthy. As cyberattacks become increasingly sophisticated, business owners and employees alike must learn to critically evaluate things we see and hear online.

Cybersecurity and the law

The dynamic and quickly changing cybersecurity landscape has brought forward new cases and scenarios that may not have been considered by lawmakers in the past. There are several areas of interest that businesses should watch closely:

- Whistle-blowers and 'hacktivists' – these groups infiltrate and leak sensitive data without prior consent, but act in the interest of free speech, human rights, and freedom of information movements.
- Legal gaps – How will the law adjust to incorporate changing technologies? For example, in 2000, the creators of the ILOVEYOU worm avoided conviction because there was no law around computer misuse in the Philippines at the time of the attack.
- Cyber insurance – more businesses are taking out cyber risk and liability insurance, which alongside financial compensation, also offers breach management and reputational protection. However, the terms on which these policies are drafted are subject to debate – there is currently an intense legal battle surrounding a 'war exclusion' clause in relation to the Russian-backed NotPetya cyberattack.

The threat landscape is continually evolving, and lawmakers will need to adapt quickly if they want to keep up. Otherwise, they risk being left behind, or worse, leaving businesses exposed to future cybercriminal activity.

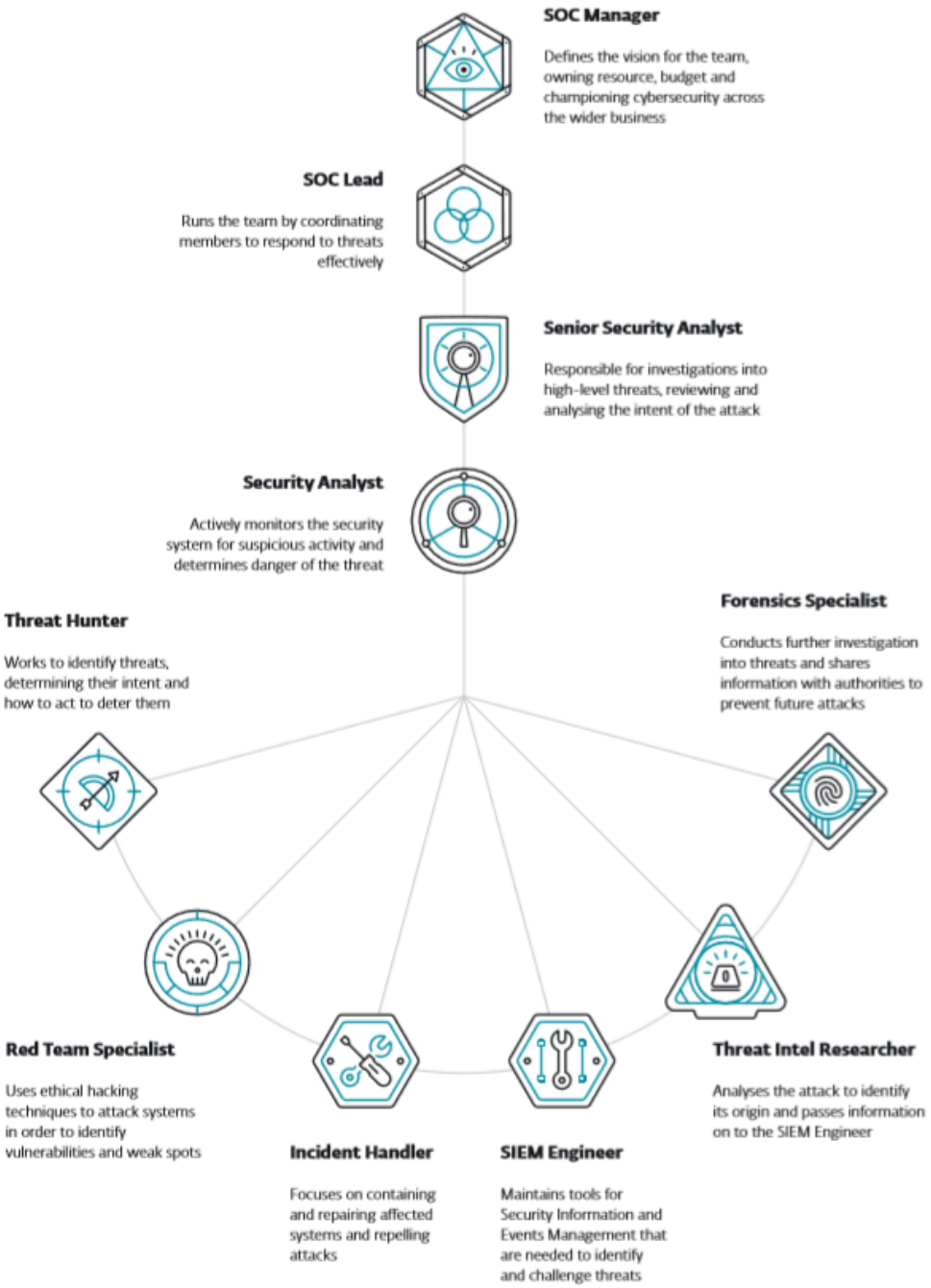
How Can Businesses Future-Proof Their Cybersecurity Measures?

The role of the cybersecurity team

Most businesses either manage their cybersecurity capabilities in-house or outsource tasks to an external team. The extent of what is outsourced varies between companies; this can range from software installation to complete reliance on an external cybersecurity provider.

However much has been outsourced, it is still important for your businesses to put together the right team for the job, particularly when it comes to reporting lines. Hiscox found that 95% of large firms have a Head of Cyber Security or Chief Information Security Officer (CISO), while the UK Government's survey revealed only 42% of businesses have staff dedicated to information security.

Cybersecurity Team Structure



Another factor to consider is the relationship between cybersecurity and IT. Although they often operate in the same department, they have different priorities when it comes to how a business handles its information. There needs to be a clearer distinction between the two, and the ISACA says that this lack of clarity can have a significant impact on a business' cyber threat defences: "This mentality can lead to disaster in the long term and [a] lack of confidence in an enterprise's cyberreadiness."

What can businesses do to protect themselves?

The threat of a cyberattack is more likely than ever before, and people clearly understand this – but how many businesses can say they know how to react when it actually happens?

Research suggests that many senior executives seem unaware of the business' day-to-day cybersecurity practices. Startlingly, 34% of businesses only update their directors or trustees on cybersecurity efforts once a year, if at all – and only 38% of employees are confident that their board of directors can read a cybersecurity report as easily as a financial statement.

If it isn't already, cybersecurity should be a key part of the business strategy, and part of making this happen involves raising awareness of issues with senior stakeholders. This may sound like overkill to many boards, but Davey Winder, Senior Contributor at Forbes stresses the importance of taking a holistic view:

> "Unless a fully 360 degree view of breach impact is undertaken then the business will suffer. Skimp on the security investigation and auditing and there may well be malicious code and backdoors left on and into your systems for threat actors to exploit again. Skimp on the security updates and the staff training and ditto. Skimp on the incident response handling and your costs will rise exponentially."

With that in mind, these are some useful first steps you can take:

- Identify top risks and threats – You probably already have the data available to assess the biggest cyber threats and where they might strike. This also encourages the team to consider any direct or indirect consequences, which helps create a more effective cybersecurity response.
- Invest (but be reasonable with budgets) – There has been a notable increase in cybersecurity spending this year, rising from $11.2 million to $14.7 million. However, the budget will never be big enough to cover all cyber threats and risks – a better solution is to invest in risk-mitigation instead.
- Build an intelligence-driven approach – The majority of businesses (77%) believe they have an effective cybersecurity team, but only 27% of the wider team have received cyber security training. Given that the insider threat is a major concern for managers, a holistic approach is essential if businesses want to defend against cyber threats effectively.
- Get the basics right – Even the simplest attacks can be successful if your business doesn't have the fundamentals in place. This can be as easy as ensuring all your software is up-to-date, or running cyber threat simulations in the same way you would practice a fire evacuation drill.

What are the authorities doing about it?

The National Crime Agency recognises that there is a discrepancy between the seriousness and scale of cyberattacks compared to the number of cybercriminal convictions. Part of the government response is to collaborate with law enforcement organisations across international borders, as well as looking at the crime network as a whole.

At a local level, the National Police Chiefs' Council is working to establish cybercrime units in every force in England and Wales, helping businesses to develop effective incident response plans. Detective Superintendent Andrew Gould, the National Cybercrime Programme Lead says this service will focus on helping victims, and deploying targeted local cybercrime prevention, in order to effect change from the ground up.

Conclusion

Prevention is better than cure

Ultimately, the most important thing you can do to defend your business against cyberattacks is to be prepared. Having an incident response plan that is well rehearsed and regularly updated could be the difference between mitigating a cyberattack and making the situation much worse.

In the next few years, developing a proactive and preventative cybersecurity strategy will be essential for any business. This includes establishing a broad awareness of potential cyber threats, combined with regular health checks, cyber risk assessments, and audits (both internal and external). However, Holly Andrews, Managing Director at KIS Finance stresses that the focus should be concentrated on your employees:

> "At the end of the day, you are only as strong as your least informed employee. Criminals that are capable of pulling off successful cyberattacks are smart - they know how to find the weaknesses in your system and how to use them to exploit your business."

Therefore, it is more important than ever before for modern businesses (and all your employees) to be clued up on their cybersecurity practices. What's more, a cookie cutter approach is no longer good enough – your strategy should be tailored to your business priorities and operations, in order to minimise the risk of becoming the next cyberattack victim.

Standing still is no longer an option

Because cyberattacks and regulations are always changing, "standing still in effect means getting worse over time." Davey Winder, Senior Contributor at Forbes says:

> "Things change quickly in the internet age, and that includes both the cyber threat and the cyber security response to it. … Those who do not take a dynamic approach to infosecurity are just treading water until they are breached - or rather, until they discover they have been."

Unfortunately, cybercriminals can currently operate with almost no repercussions for their actions. However, businesses should know they don't have to deal with this alone. The government is working to implement national measures such as a 'TeamCyberUK' as well as various international operations with the EU and beyond, which all aim to support businesses with their cybersecurity efforts.

Cybersecurity will only grow in importance and the risks will continue to increase, but Edward Whittingham, Managing Director at The Defence Works, says business owners shouldn't be intimidated:

> "Cybercrime is just the natural evolution of ordinary crime. Over time, we will start to see much more acceptance of cyber and data-risks, in the same way are all familiar with other similar risks throughout the business."