Looking beyond 2018: the future of cyber security
CONTENTS

1. Introduction ........................................... P.3

2. The changing face of cyber crime ............ P.4

3. Misconceptions about the cyber threat ... P.5

4. Profiling a cyber attacker ......................... P.6
   Why they do it
   How they choose their targets

5. Cyber security challenges ....................... P.7
   It’s a complex world
   More expertise needed
   No security culture
   The good and bad of innovation

6. The future cyber threat landscape .......... P.9
   Proliferation of mobile
   AI, machine learning and IoT
   Crime-as-a-Service
   Compliance and cyber security
   We, the people

7. Preparing for the future ......................... P.11
   Technology
   People
   Processes
   Boosting success

8. Conclusion ........................................... P.13
   Sources
   About Pulsant
   About Pulsant Protect

ABOUT THE AUTHOR

Martin Lipka is a leading cyber security expert with almost two decades of experience in the industry.

Having developed his passion for IT at a very young age, Martin was a highly sophisticated hacker in his teenage years and quickly went on to create his own Internet Service Provider (ISP) in his home country of Poland.

Martin first joined Pulsant in 2008 as a Network Manager and became Head of Connectivity Architecture in 2014 — this role involves overseeing Pulsant’s network and cyber security strategies and leading the company’s infrastructure transformation programme.

MARTIN LIPKA
HEAD OF CONNECTIVITY ARCHITECTURE AND CYBER SECURITY EXPERT
1. INTRODUCTION

Cyber security has evolved from being the stuff of Hollywood blockbuster plots, to becoming a national priority.

Global governments are taking the threat seriously, as seen in the UK's own National Cyber Security Strategy, the establishment of the National Cyber Security Centre (NCSC), investment of £1.9 million in transforming the UK’s cyber security, and the introduction of risk management frameworks such as Cyber Essentials that are designed to help businesses mitigate the threat of cyber attacks\(^1\).

Being hacked and having your data breached are no longer intangible “might happen” threats but blatant risks that organisations of all sizes are currently dealing with. In fact, there is hardly a week that goes by without the media reporting a cyber security event that has affected individuals, businesses and industry. Yet despite the prominence of the threat, many businesses are still at a loss when it comes to securing their operations from cyber criminals.

One of the main reasons for this is many of those organisations see cyber security as a destination — instead of a journey. The truth is that cyber security is an ongoing initiative that affects the entire business, its people, partners and technology.

In this whitepaper we take a broader look at the cyber threat landscape, the future implications of big data, machine learning and the Internet of Things (IoT) on cyber crime, and what this could look like, as well as how businesses can keep their staff, data, customers and intellectual property safe.

2. THE CHANGING FACE OF CYBER CRIME

Looking at the evolution of cyber crime and cyber criminals wouldn’t be complete without discussing how cyber security itself has changed. It is no longer an IT issue, but is seen as a board-level objective, with buy-in needed at all levels of the organisation.

The reason for this shift, apart from the acknowledgement of the severity of the cyber threat, is that every business is a potential target. In days gone by it was industries like Financial Services that typically paid more mind to cyber security as they were seen as the most likely targets.

Now businesses of all shapes and sizes, in all industries are at risk. This is due to the fact that setting up an attack or paying for one is easy and accessible, especially on the dark web.

Cyber criminals, for the most part, are opportunistic; they scan the internet looking for vulnerabilities to find ways into your corporate network. Of course the harder it is for them to gain access to your business, the more likely they are to exploit companies that are easier to penetrate. Importantly, cyber security isn’t about becoming bulletproof — every organisation is fallible. Instead, it is about mitigating the risk by having protection at every layer in order to block the attack chain.

The aim of any cyber security strategy is threefold:
1. Stop the attack where possible
2. Identify the threat quickly
3. Mitigate the risk

A cyber attack can be broken down into various stages, also known as the attack chain:
- **Reconnaissance** – The attacker researches, profiles your business, and tests the target environment, network and your people.
- **Infiltrate and weaponise** – The attacker breaks in and creates remote access to take position inside your organisation or target network.
- **Discover and Identify** – An attacker uses their internal position to understand more about the environment and the surrounding systems.
- **Exploit and capture** – The attacker works to persistently take control of an asset, typically information that is critical to you to exploit vulnerability.
- **Command and control** – The attacker moves the asset out, or in some cases damages or destroys the asset.
3. MISCONCEPTIONS ABOUT THE CYBER THREAT

The pressure is on… they’re looking at a blue screen with a command prompt and are typing furiously away… in 30 seconds they’ll have breached your firewalls…

This is the typical representation of a cyber attack in popular culture. The truth is a little different and leads to the first misconception — hacks don’t happen in minutes. It takes time to breach an organisation, to find a way in and exploit that gap — just take a look at the attach chain on page 4.

Another misconception is that attacks or breaches are noticed immediately. This is not the case at all. Yahoo, for example, experienced a massive data breach in August 2013 in which 1 billion customer accounts were affected. But the company took three years to find the breach and then disclose it, and four years to complete the actual investigation (which revealed that in fact 3 billion accounts were affected)².

While not all instances are that extreme, figures in the Ponemon 2017 Cost of a Data Breach Study suggest that US companies take 206 days to find a data breach³. Other research suggests that European companies are taking even longer — 469 days on average⁴.

When a breach is reported there are generally two reactions: that hacker is a genius; or the company has poor security. The common misconception is that the hack or breach is down to the skills of the perpetrator. Not so. All too often attacks are successful because businesses don’t have a cyber security strategy and the appropriate defences in place.

Another misconception about cyber security is that when it comes to the cloud, protection is a given. While you might recognise it’s your responsibility to secure data in your organisation, once it goes to the cloud it becomes the cloud provider’s problem. Right? Wrong. Your data is always your responsibility. The fact is that cyber security is the job of everyone involved. Your cloud provider protects its infrastructure and you as its customer, but it is up to you to make sure you have the processes and procedures in place to keep your data secure.

² https://www.wired.com/story/yahoo-breach-three-billion-accounts/
³ https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/
4. PROFILING A CYBER ATTACKER

She’s sitting behind a bank of screens, surrounded by empty cans of Red Bull and pizza boxes… this is the person responsible for bringing down a major pharmaceutical giant…

Ninety-five per cent of attacks are perpetrated by amateur hackers who simply use known vulnerabilities to exploit the weaknesses in company systems.

As a result, protecting your organisation from these hacks could be as easy as ensuring your patches are up to date and that your IT department is keeping your anti-virus software current.

However, for the remaining 5%, the outlook is a little different. Hackers supported by the state or those involved in corporate espionage make up another 4% and their skills are typically much better than the 95%, which makes it more difficult to protect against them. The last 1% lurk behind the scenes and are rarely seen in the fray of attacks. Instead, this small percentage of cyber criminals focuses on identifying vulnerabilities and providing other hackers with the means to actually carry out the attacks. The WannaCry event of 2017 in which the ransomware worm attacked computer networks on a global scale, including the NHS, by exploiting a Windows vulnerability5 was one example of this.

WHY THEY DO IT

Aside from the skills involved in cyber crime, what are the typical motivations for these attacks?

Money is, of course, one of the overriding objectives. Whether that is stealing valuable data and holding it for ransom, selling it to a third-party or being hired specifically to perpetrate an attack, the driver is often commercial.

Cyber crime is a booming industry — crime-as-a-service or rent-a-hacker services are now commonplace. In the past you would have to venture into the dark web to seek out a hacker. Take Distributed Denial of Service (DDoS) attacks as an example; you can order such an attack for the equivalent of $50 per day6 or use the surface web to order up an attack on popular website Fiverr, for, you guessed it, a fiver7.

Other reasons include hacking based on beliefs or ideology; for fame and attention; for political reasons; or to exact revenge. Regardless of the reason, the consequences of hacking are far-reaching and the impact on businesses — loss of revenue, and loss of customer and market trust — quite significant.

HOW THEY CHOOSE THEIR TARGETS

There are a number of ways that cyber criminals select their victims, depending on their motivations for the attacks. The key thing for you to remember is that while your business can never be completely bulletproof, you should never make it easy for hackers to get what they want.

Low hanging fruit
Many attacks are opportunistic. Hackers use automated bots to scan and assess the current online surface of any business connected to the internet, searching for known vulnerabilities. The result is a list of global internet assets that the hacker can prioritise based on factors like anticipated financial success, security status of the company and the willingness to pay.

Recurrent ransom attack
Hackers actively share or sell intelligence about their successful blackmail campaigns. As a result, other hackers will capitalise on this information and try to extort money from those same victims based on their vulnerability and willingness to pay ransom.

Phishing
Attackers will randomly infect parts of vulnerable or unpatched infrastructure in order to use these machines as “zombies” in a bigger attack on another target. These zombies are also a source of revenue for hackers and are traded online.

Hacktivism
These targets are chosen based on the hackers’ political, social or ideological beliefs. Hackers can work alone or with a group of other individuals to achieve a common goal, related to civil disobedience, free speech, human rights, anti-capitalism, etc.

Supply chain
The hacker is unable to attack a target head on, due to strong defences, for example. Instead, the hacker will research the target’s partners and attack through a smaller, less secure company to gain access to the intended target.

Corporate espionage
Hackers are contracted to steal an organisation’s confidential information or intellectual property by a competitor.

---

1[https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html]
2[https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/]
3[https://www.tripwire.com/state-of-security/featured/hire-a-ddos-attack-for-as-little-as-5/]

Find out how we can help your organisation:
call 0345 119 9911

pulsant.com
5. CYBER SECURITY CHALLENGES

As well as the ever-changing and rapidly evolving cyber security landscape, there has also been a major evolution in the sophistication of business infrastructures and systems, as well as the ways these are accessed by individuals.

For example, it’s no longer as simple as it used to be to secure an office network — with people often working remotely, and many businesses taking advantage of hybrid models where their systems are decentralised — what was once a simple task is now far more complex.

The most common barriers are budgetary constraints, confusion around cyber security, and lack of alignment between technical and human efforts. There are, however, many more challenges to be addressed.

IT’S A COMPLEX WORLD

Most businesses today are undergoing transformation of some kind, driven by the continued adoption and use of cloud, and other digital technologies. This attitude of innovation is also evident in the cyber defence offering on the market. As hackers get more sophisticated, so too do the tools we use to fight them; it’s a never-ending circle that is driven by that innovation. The cyber security market is growing at pace with research suggesting that it will reach £163.17 billion ($231.94 billion) in 2022, growing 11% year on year from 2017.8

What this effectively means is a flood of security vendors on the market, all offering a number of products. While choice is always good, given the sheer size of the market, how do you wade through these options and choose the best ones that match the needs of your organisation? Yes, multiple tools are needed to provide protection at different layers but all too often the result is that organisations are using multiple products to cover different areas of operations. The danger here is that these solutions are not properly co-ordinated or integrated, and the data generated is brought together manually, which is time consuming and can be inaccurate.

This level of complexity makes it all the more difficult for businesses to keep themselves secure. In addition, hackers are fully aware of the number of products on the market and the number of solutions a company typically needs.

MORE EXPERTISE NEEDED

One of the main challenges in cyber security is that organisations have a lack of knowledge when it comes to understanding their threat surface and security gaps. This is often due to the lack of in-house expertise — and the widening skills gap in the cyber security sector. This makes it difficult to hire and retain the right staff.

This acknowledged skills gap is only widening. According to the (ISC)2 Global Information Security Workforce Study, in the next four years there will be a shortage of 1.8 million cyber security workers.9 Apart from this overall lack of relevant skills, there is also a shortage of specific skills inside of organisations. IT staff don’t necessarily have the level of expertise needed to help protect the organisation. In addition, there is also a lack of understanding at board level about the cyber threat, which results in an incomplete (or completely absent) cyber strategy.

Hackers are well versed in finding ways around these solutions and capitalising on the gaps and vulnerabilities that still exist.

---

8 https://www.marketsandmarkets.com/PressReleases/cyber-security.asp
NO SECURITY CULTURE

Cyber security requires an organisation-wide commitment and should be driven from the top down. Management support is crucial in cyber security, from allocating budget and resources, to recruiting the right staff. Importantly, there is a definite lack of security culture within the modern organisation, regardless of its size or the industry in which it operates. This should be addressed by meaningful training and educating of staff on the methods used to infiltrate companies by social engineering.

According to most research, people are the weakest link in the cyber security chain, even in organisations with the most mature defence. As a result, staff need to understand their role in cyber security (for example, downloading attachments, checking the identity of email senders, and being aware of social engineering tactics), as well as the consequences of getting it wrong.

Looking at phishing as an example, attackers know that people are the weakest link and exploit this through digital impersonation. A key tool for attackers is the business email compromise (BEC) scam.

These scams are on the rise. In fact, 96% of businesses have been targeted by these attacks, with companies experiencing 45 attacks in a six-month period, according to research\(^\text{10}\).

SOCIAL ENGINEERING

This is a method that uses deception to get people to inadvertently help attackers. It is a growing problem and is especially threatening as humans are regarded as the weakest link in the cyber security chain.

THE GOOD AND BAD OF INNOVATION

Cyber security innovation is leaping forward at a tremendous pace. While this benefits organisations, it is more advantageous to cyber criminals. This is because attackers are more agile in their approach and can act quickly, whereas businesses are hindered by a number of issues, including inadequate or disjointed processes, lack of awareness or understanding of the risk of impact, and a lackadaisical attitude.

\(^\text{10}\) https://www.helpnetsecurity.com/2018/02/01/bec-scams-surge/
6. THE FUTURE CYBER THREAT LANDSCAPE

Looking ahead, the top three technological advances likely to impact the cyber landscape are the increase in use of mobile, advances in artificial intelligence (AI) and the increasing popularity of IoT.

This, coupled with the burgeoning business model of crime-as-a-service, means that cyber attacks are only set to increase.

PROLIFERATION OF MOBILE

There is little doubt that the invention of the smartphone has changed our lives from both a business and personal point of view. We are always connected, able to navigate to new places, chat with colleagues, collaborate on documents and find out any information through the use of an application or by searching the web. The idea that we have the world in our hands has never been more true than when it comes to the use of the mobile phone. While the physical device may be in our hands, it connects us, our data and our information to sites all over the world therefore increasing our personal attack surface.

Just imagine, for example, the very real possibility that hackers gain access to the data and information on our smartphones by exploiting a vulnerability in a public WiFi network. This could happen without us even realising that we’ve suffered from a breach until it’s too late.

In 2018 and beyond, it is expected that major breaches and attacks will take place on mobile as hackers fully realise the potential of your phone to gain access to your personal and work resources. According to the Symantec 2018 Internet Security Threat Report, there was a 54% increase in mobile malware variants in 12 months. More than that, the security company said it blocked 24,000 malicious mobile applications every day in 2017.

AI, MACHINE LEARNING AND IOT

Advances in AI and machine learning will transform the cyber threat landscape in unpredictable ways and will change the way businesses and cyber security professionals view the industry. From human-to-human/attacker-to-victim techniques, the cyber security landscape might turn into machine-to-human/attacker-to-victim or machine-to-machine/attacker-to-victim relationships. What is predictable, however, is the fact that attack vectors and campaigns will become increasingly sophisticated even as organisations tighten defences.

When it comes to IoT, the threat surface increases exponentially. Gartner predicts by 2020 there will be 20.4 billion endpoints connected to the internet, each potentially presenting a way into a home or organisation. These devices could also be used as zombies or jump off points by hackers in different campaigns.

In a recent article, Ondrej Vlcek, CTO & GM of Consumer at Avast, paints a picture of a future where AI technology is a double-edged sword from a security perspective. “The availability of low cost computing and storage, off-the-shelf machine learning algorithms, AI code and open AI platforms will drive increased AI use by the good guys to defend and protect — but also increase deployment of AI by the bad guys. There will be sophisticated attacks launched at a grand scale, quickly and intelligently with little human intervention, that compromise our digital devices and web infrastructure.”

---

12 https://www.gartner.com/newsroom/id/3598917
13 https://www.futureofeverything.io/future-of-cybersecurity/
CRIME-AS-A-SERVICE

The commercialisation of hacking services is growing in popularity and will continue to do so, driven by the presence of poor cyber security strategies, the opportunistic nature of hackers and the ideal environment that DevOps presents them with. This perfect storm lowers the barriers to entry for cyber crime and, in effect, makes it more affordable and easier to find for anyone with an internet connection. Individuals no longer have to trawl the dark web looking for the services of hackers — they only need to browse the surface web in order to contact one of these individuals, give them orders and pay them for their services.

COMPLIANCE AND CYBER SECURITY

Organisations in heavily regulated areas, such as financial services and pharmaceuticals, understand more than most the importance of compliance. In today’s business environment, more industry frameworks are being applied and not just for the likes of banks, law firms and insurance companies. Consider, as an example, the European Union’s General Data Protection Regulation (GDPR) which applies to all businesses. The regulation relates to the processing and storage of personal information and all companies must comply — even if they don’t actually hold any of this data.

While being compliant doesn’t necessarily mean a business is secured, if you are secured, in all likelihood you are compliant and it will be the non-compliant companies that will make the more attractive target for ransomware attacks and breaches, especially given the hefty fines associated with GDPR.

WE, THE PEOPLE

The human element is widely acknowledged as the main issue when it comes to cyber security. In fact, according to The Institute of Information Security Professionals (IISP), 80% of security professionals see people as the industry’s biggest challenge14. While this covers both the skills gap and the role staff unwittingly play in cyber attacks, it demonstrates the scale of the problem. And it is hardly likely to change.

80% of security professionals see people as the industry's biggest challenge

7. PREPARING FOR THE FUTURE

Cyber security may seem daunting, but protecting your organisation, your customers and your data isn’t an impossible task. Typically, the best approach is a holistic one that addresses three main areas: your technology, people and processes.

TECHNOLOGY

While the use of technology in the fight against cyber crime is important, it is equally important to limit the number of security tools you use. Instead of quantity, look for quality. When it comes to the data that is generated by these tools employing AI and machine learning to analyse it and seek patterns can be critical in protecting your organisation. AI will provide more granular visibility of the threat affecting your business enabling you to uncover more complicated threats.

In addition, while some areas of your business may be more vital than others, they should all be protected. If you are not securing everything you are, in effect, securing nothing. As a result, your organisation should aim for security-by-default or have a security-focused culture where being secure in everything you do becomes standard. This will become easier going forward because with the current software-defined—everything approach, the capabilities to deliver cost-effective technical solutions will only increase. In the same vein, where attackers are using code as a weapon, this capability will allow you, your security team and security partner to actually use code as part of your defence strategy.

The adoption of increased automation and orchestration, as well as the use of DevOps environments will also be key tools used to make your cyber defence strategy more agile, cost-effective and make your organisation harder to compromise as these elements largely remove the human factor from the equation.

Finally, cloud also has a role to play in cyber security. Security was long regarded as one of the main barriers to cloud migration and increased cloud adoption. However, as the technology has matured, this concern has been addressed. In fact, organisations with virtualised infrastructures may even be more secure than traditional on-premises environments.

The reason? These cloud environments — if properly secured by both the organisation itself and the cloud provider — are maintained by highly skilled professionals whereas businesses may not have those particular skills in-house to maintain and secure their infrastructure, nor do they have the time needed to dedicate to this task.

PEOPLE

Building on the idea of security-by-default, it is important to build cyber security culture into your organisation and emphasise its importance by having it driven and supported at board level. Your people have a vital role to play because technology cannot function alone — it needs a level of human interaction.

Education will be important here too — not just in terms of making all employees aware of the importance of security, their role in maintaining it and the consequences of getting it wrong, but also in upskilling and educating security personnel. If you are working with a managed security service provider, you can take advantage of their skills base to boost the quality and speed of your in-house security team.

It is also critical to keep your entire organisation up to date on the cyber threat, that is making them aware of new threats, new methods of infiltrating organisations and the latest social engineering methods being employed.
PROCESSES

Your processes are key to implementing an effective cyber-security strategy. This includes activities, roles and documentation used to mitigate risks. Here you can leverage the skills of your key security stakeholders and partners to develop a list of meaningful policies, procedures, standards and guidelines that should be accepted and respected by your staff, and based on the required compliance, laws and regulations.

These processes are useless unless controlled by technology and followed by your staff. Having an embedded security culture will help you in making the approach a reality.

BOOSTING SUCCESS

Integral to the people, processes and technology approach are a number of other things you can do to ensure success.

Partner with experts
When it comes to cyber security, you can’t necessarily do it alone. And you shouldn’t have to. If you work with a trusted partner you can benefit from their industry knowledge, in-house skills and the large investment they have made into all areas of their business. This collaboration can help you boost your skills, knowledge and experience.

Take a risk-based approach
By knowing your business extremely well, understanding your attack surface, the defences but most importantly the gaps, you can prioritise your risks around the three areas of technology, people and processes. Hackers will only be able to exploit your organisation if they notice something that your risk assessment failed to identify.

Pay attention to even the smallest risks, threats and violations as part of your ingrained cyber security culture because if left unchecked, these provide the hacker with the first thing they need, a way in.

Breach! Breach!
Your organisation, in fact no organisation, will ever be bulletproof. It is important to take an ‘assume breach’ approach, this mindset drives operational design and practices to develop better response strategies. As a result, you will at some point face a cyber security incident — the severity of which will be determined by your preparedness and the processes you have in place to mitigate the risk. Embrace the “chaos monkey” philosophy in which you continuously test the resilience of your cyber defence in simulated cyber battles.


How to avoid becoming a cyber security statistic

- Be proactive; assume that you will be attacked
- Get cyber security on your board’s agenda
- Think like a hacker; test your defences regularly
- Lean on security partners for support
- Implement a cyber security culture
8. CONCLUSION

The cyber security threat is one that businesses are beginning to take seriously. And rightly so — cyber criminals and their attack methods are becoming increasingly sophisticated, using a combination of technology, expertise and social engineering to reach their hacking goals.

It’s important to remember that just as no company can be 100% safe, hackers are not necessarily all geniuses who are infallible. In the same vein, making a significant investment in technology from a vendor who’s promised 100% cover could lull you into a false sense of security or make you believe that it won’t actually happen to you. In effect, keeping your organisation safe and mitigating the risk of an attack or breach is achievable. But how? It begins with the right attitude — an acknowledgement of the threat and fostering a security-orientated culture within your business.

From there it’s all about developing a sound cyber security strategy that addresses the three important elements of people, processes and technology. This approach needs to be supported and driven by the board and top management in order to be successful.

In addition, there is no need to tackle cyber security alone. Working with a trusted partner, such as a managed service provider, can be beneficial in overcoming internal challenges, such as budget constraints and lack of skills, and in formulating a cyber defence and response strategy. Working with such a partner will become even more important going forward because of the speed at which the landscape is changing. It is near impossible for any one individual or company to possess all the skills and expertise needed, so relying on a partner to complement your own skillset will be crucial.

Ultimately, the cyber threat landscape will continue to evolve and businesses, security professionals and the defence technologies will need to keep pace in order to deal with the risk hackers and cyber criminals pose.

SOURCES

   center/threat-report
ABOUT PULSANT

Pulsant is one of the UK’s leading providers of hybrid cloud solutions with a core focus on private and public cloud services, network connectivity, security and integration.

With more than 20 years of experience in the industry, we serve more than 4,000 customers in the private and public sector across a variety of industries. We hold a number of accreditations, including ISO27001, PCI DSS and BSI CSA Star for cloud security. We are also on the G-Cloud framework, and were awarded the Royal Warrant as a provider of hosted IT and datacentre services to the Royal Household.

ABOUT PULSANT PROTECT

Pulsant Protect is our dedicated security offering that covers your entire business, from your people and your network, to your cloud infrastructure and your applications. As a managed security provider we use our own expertise and relationships with industry-leading security specialists to deliver a comprehensive solution that meets your needs, designed to reduce cyber risk, meet compliance requirements and give you greater visibility across your IT estate.

OUR SOLUTIONS INCLUDE:

Surface Protect
Challenges your existing protection to identify any goals and areas to improve on, including your people, processes and technology.

Cloud Protect
Simplifies the security of your infrastructure and applications by offering a single solution that can be deployed across all supported platforms.

Internet Protect
Is a set of cyber-security elements that protects your business from disruption reputation damage and fraud.

Office Protect
Is a set of unified, complete and agile security controls, that encompasses access, email, malware protection, and filtering of content and information.

Download our brochure

Find out how we can help your organisation, call 0345 119 9911 or visit www.pulsant.com