BOOST REDPAPER - *Summer 2018*

Cyber Security 101: The Definitive Executive eBook

Exclusively relevant for EVERY Cyber Security Reseller, MSP, MSSP, and SI Executive.

BOOST
TECHNOLOGY GROUP

Boost Performance Report

INDEX

Section One: **Market Overview and Stats** page 5

Section Two: **Identifying the Players** page 6

Section Three: **Pressing Security Threats** page 8

Section Four: **The Technology Minefield** page 11

Section Five: **Obstacles for Customers** page 13

Section Six: **Channel Challenges** page 14

Section Seven: **Conclusion** page 15

Clearing the security minefield

What exactly does the security market look like today and what are the threats corporates are facing? This report will breakdown the market in terms of main players, threats and solutions, examining the challenges facing both suppliers and customers as they battle against a common enemy – the Cybercriminals.

Cybersecurity is currently the hottest ticket in town, and with the constant threats and security challenges facing modern businesses, having the right solutions in place is going to be a priority for the foreseeable future.

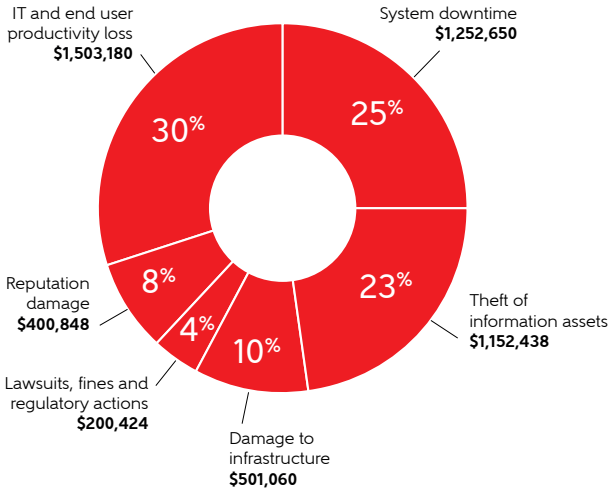
According to the Ponemon Institute, seven out of 10 firms it questioned in 2017 said their security risk 'increased significantly' that year, and it also estimated that the total cost of a 'successful' cyber attack is over $5m, equivalent to $301 per employee. *(See pie chart)*

But with the growth in ever-complex threats facing businesses there is a downside, and that is the sheer number of security companies and solutions playing the market, and with the growth of the cloud, do customers want an on-premises or cloud-based solution? There is almost an endless list of possibilities and associated costs. Customers are completely confused over where to turn and which solution/ vendor and strategy to actually use.

This is where their trusted IT reseller comes into play, but even these experts are faced with a plethora of choices when it comes to nailing colours to the mast. Where should they actually turn?

In this report, we will look at the state of the security market, the current threats companies are facing, examine some of the leading players and technology trends, and also delve into what the challenges faced by both customers and suppliers actually are and how they can be potentially overcome.

Cost of endpoint attacks



Source Ponemon Institute:
https://blog.barkly.com/2018-cybersecurity-statistics

Section One: Market Overview and Stats

Figures on the state of the security market are seemingly released every day and vary quite considerably – so it is very difficult to get an accurate prediction of just how much will be spent in the coming year.

However, the one thing all analysts and market watchers agree on is that spending is increasing exponentially and that will continue for many years to come.

For instance, market watcher IDC, predicts global spending on security-related hardware, software and services will reach $119bn by 2021 *(Source 1: Worldwide Semiannual Security Spending Guide)*. And it added that with nearly every industry investing in security solutions to meet a wide range of threats, spending is expected to achieve a compound annual growth rate (CAGR) of 9.6 per cent between 2016 and 2021.

Sean Pike, program vice president for IDC's security products and legal, risk and compliance programmes, said: "Three overarching trends are driving security spending: a dynamic threat landscape, increasing regulatory pressures and architectural changes spurred by digital transformation initiatives.

"Organisations are actively searching for product and service efficiencies that maximise spend in order to fully address such complex challenges," he added.

However, other figures from Grand View Research *(Source 2)* anticipate the market will reach $167bn by 2025, as increased competition drives the need for automation in multiple markets. And with automation, comes an increased need for security solutions. An increase in infrastructure around the globe has also resulted in an increased demand for safety systems such as access control systems and video surveillance for real-time monitoring. And security surveillance, it predicts will be one of the fastest growing areas of investment.

Breaking it down, figures for the European cybersecurity market are also widespread, but Mordor Intelligence *(source 3)* has predicted the European market will reach $41.3bn by 2020, a CAGR of 19.8 per cent.

Gartner predicts the security market will be worth $96bn in 2018 *(Source 4)*, fuelled by increased regulation, a shifting buyer mindset, awareness of emerging threats, and digital business transformation.

Ruggero Contu, research director at Gartner, said: "Overall, a large portion of security spending is driven by an organisation's reaction towards security breaches, as more high profile cyberattacks and data breaches affect organisations worldwide. Cyberattacks such as WannaCry and NotPetya and the Equifax breach (and more recently Meltdown and Spectre) have a direct effect on security spend because these types of attacks last up to three years," he said.

Despite the variation in predictions, the central message remains the same; security spending is on the up. As we shall see in Sections five and six of this report, that is good news for the channel, but it also means a lot more work for channel players.

Section Two: Identifying the Players

With the positive news that security spending is increasing, it also means the number of security companies are multiplying, with new players entering the market on a regular basis. But this is not always good news or a welcome development with the dial swinging very much back to the more established players.

In fact, at the 2018 InfoSec show in London, the vibe was very much that security start-ups were becoming more unwelcome *(Source 5)* as often they attract VC money because of their cutting-edge technology, but many fail to have a proper business plan in place and actually make an impact on the market, therefore proving a risk to any partners that may invest time and money in their offerings.

So, with start-ups out of the equation – the question is, who are the main players on the security stage. There are tens of well-known names working with both business customers and consumers. Below is a sample list of some of the most recognised names in the security market today, and all of them are vying for the same customers and partners. It is no surprise that the market is so cutthroat.

Amazon Web Services: Cloud-powered security offerings covering security, identity and compliance

Barracuda: Specialising in email protection, network and application security, data protection, threat detection and analysis and more.

Cisco Systems: The networking giant is investing heavily in security, with CEO Chuck Robbins stating that it will be making more acquisitions to add security features to its portfolio. Its products integrate security across the network, cloud, internet, email and endpoints.

Check Point: Unified Threat Management (UTM) specialist, providing solutions on network, mobile, and cloud, along with security management services.

CyberArk: Israæli security player specialising in identity and Identity Access Management (IAM) offerings or Privileged Access Security according to its website. Claims more than half Fortune 100 companies use its offerings.

Dell EMC: Four-pronged security portfolio covering data protection, identity assurance, threat detection and response and unified endpoint management.

FireEye: Covers enterprise security solutions ranging from network to email and threat intelligence solutions.

Fortinet: Specialises in network and content security along with secure access products.

HPE: Offers a Secure Compute Lifecycle to protect enterprises from malicious threats.

IBM Corporation: Has one of the broadest security R&D operations and owns over 3,000 security patents globally. Its enterprise IT security suite covers mobile, data, network and endpoint solutions, and Big Blue uses AI and cloud platforms to guard against and detect threats.

Intel Security: Focuses on hardware enabled security capabilities encompassed directly into the silicon. Suffered a massive setback in 2018 when vulnerabilities on its chips were discovered that left users vulnerable to hackers. It affected most of the Intel-powered computers in use and the firm has a huge sum of money set aside to cover compensation.

Kaspersky Lab: Russian giant covering threat management, hybrid cloud security, endpoint security, industrial cybersecurity and fraud prevention among others

McAfee: Reborn after being spun off by Intel. Covers endpoint security, threat prevention, web control, threat containment and more.

Microsoft: Offers a huge range of security offerings from its Windows Defender product to its cloud- based Azure and Office 365 security compliance centres. It has pledged to invest $1bn annually into security.

Mimecast: Email security, threat protection/detection, security messaging, encryption and more.

Palo Alto Networks: Three-pronged security platform covering next generation firewall, advanced endpoint protection and threat intelligence cloud.

RSA Security: Huge portfolio covering advanced threat detection, SIEM, endpoint protection, network monitoring, ATP and more.

Symantec: Offers huge range of security solutions including advanced threat protection, email security and cloud and network security services. It also runs AV software giant Norton.

Sophos: Another mammoth range of products covering endpoint security, encryption, network security, email and mobile security and much more.

Trend Micro: Another large portfolio covering hybrid cloud security, network security, email security. ATP, Intrusion prevention and much more.

With the above being just a fraction of the names available to work with and sell in the market, it is little wonder that some customers and partners are left confused as to which direction to turn. *More on this point in section 5 of this report.*

Section Three: Pressing Security Threats

Threats are increasing on a daily basis as cybercriminals launch evermore complex attacks and attacks that can penetrate even the toughest of armour if a company is unprepared.

According to research by specialist security website Cybersecurity Ventures *(Source 6)*, cybercrime will cost the world $6tn (trillion) annually by 2021, up from a 'mere' $3tn in 2015, and will be more profitable for the criminals than the global trade of all major illegal drugs combined.

These costs, the site claims, include damage and destruction of data, stolen money, lost productivity, theft of intellectual properly, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems and finally reputational harm.

And with six billion internet users predicted by 2022 and more than 7.5 billion by 2030, there are a whole lot more potential perpetrators and victims to come.

In the words of **Robert Herjavec**, founder and CEO at Herjavec Group, which sponsored CyberSecurity Ventures' research: "The risk is very real, and we can't allow ourselves to be lulled into a sense of inevitability. We all have a role to play in how we protect our businesses from the accelerating threat of cybercrime". So, what are the type of threats companies are facing, and what should they be looking out for?

Listed below are just some of the most prevalent and complex threats facing both consumers and corporates alike, but just as the security space changes and evolves, so do the number and type of threats on an alarmingly regular basis. Much like caging water, keeping count of the number of different threat variants out there is pretty much impossible.

'Fileless' attacks: According to Ponemon Institute – 77 per cent of attacks that compromised organisations in 2017 used fileless techniques and in 2018 a third of all attacks will use this method. Criminals are moving away from using malicious .exe files to deploy malware, using a technique that bypasses traditional security solutions such as anti-virus, which rely on analysing executable files to make threat detections.

Cryptomining or Cryptojacking: Criminals hijack a computer's CPU power to mine cryptocurrency directly, without the target even being aware any cryptomining malware has been dropped. According to security vendor Check Point, cryptominers impacted 55 per cent of organisations globally in 2017.

Crime-as-a-Service: It is not just IT suppliers or managed service providers (MSPs) that have a service to offer customers *(Source 7)*. According to an article by CSO, criminal organisations will become increasingly

sophisticated and just like legitimate businesses collaborate to win new business, or provide a complete service, so will these underworld organisations. And their methods will get cleverer and more complex over time.

IoT security: As more and more companies embrace IoT and deploy more devices on their networks, creating more endpoints, they are laying themselves open to more risk by giving attackers access to their data via these devices, that are often poorly secured or completely unsecured. Companies will find it increasingly difficult to know what data is leaving their networks or being secretly captured and transmitted by devices such as smartphones and smart TVs. This ties in with BYOD. See below:

BYOD: This gœs hand in hand with IoT. Employee flexibility is becoming a key requirement for firms of all sizes, and with that comes a growth in the trend to bring your own device to work, again meaning more endpoints are created. According to Gartner *(Source 8)*, more than half a billion 'wearable' devices such as smartwatches, head-mounted displays, wristbands, Bluetooth headsets, fitness monitors and sports watches, will be sold by 2021. See also Mobile threats, below.

Mobile threats: As smartphone adoption continues to grow - IDC predicts there will be 1.9 billion smartphones in use globally by 2022 *(Source 9)* – so will the rise of mobile threats – both at a consumer and a business level. Banking Trojan and mobile ransomware will be the biggest threats to mobile systems *(Source 10)*.

Ransomware: The WannaCry attack brought the UK's National Health Service to its knees in 2017, and affected computers in over 150 countries. And the threat is not going away. In 2018, experts believe cloud computing businesses which house the data for their customers, are top of the hitlist *(Source 11)*. Giants like Google, Amazon and IBM have hired teams of experts, but the smaller companies that perhaps don't have that kind of financial firepower, will be especially vulnerable.

Supply Chain Weakness: At every point in a supply chain are weak spots. The point at which valuable and sensitive information is shared with suppliers and partners, means control is often lost and that data is at a greater risk of falling into the wrong hands or being compromised. Securing every point of the supply chain should be a priority.

RDP (remote desktop) vulnerabilites: While the concept of RDP is a good one, there are many ways unscrupulous criminals can get access to a desktop in a supposedly encrypted session. Many firms forget to install updates, leaving their networks at risk.

Phishing/Vishing/Smishing: These are all legitimate terms used by fraudsters to convince people – both consumers and corporate users - to share sensitive data/hand over money, or download something that will infect their computer. No user is safe from these type of attacks. And this leads to:

People/Employees: Poorly educated employees are definitely one of the biggest threats to a company today. Unless they are properly trained in how to ignore potential viruses, phishing attempts etc by clicking on links, or can see a threat simulation firsthand, they will continue to put company data at risk. Many will carelessly share sensitive data either maliciously or without thinking through the consequences. This is also backed up by many research reports. For example, figures from Egress Software Technologies last year revealed that around one quarter (24 per cent) of UK employees admit to intentionally sharing confidential business information outside their organisation, often to competitors or new and previous employers.

CEO fraud/ID Theft – also known as 'Spear Phishing': A popular form of fraud by cybercriminals that will happily impersonate a CEO/FD or C-suite exec, either on the phone or via email to customers; claiming they are due a payment, or a payment has not come through, or they need the customer to click on a link, or share payment/sensitive information.

Section Four: The Technology Minefield

There are literally hundreds of different security technologies available on the market, and it is virtually impossible to become familiar with every single one. The key to staying secure is selecting the right combination of technology sets, or adopting the right general approach to security for a particular business need. No two companies have the same requirements.

As we shall see later in the report, this is a task that the channel has taken head-on, as more customers demand a tailor-made security strategy that covers their every need.

The days of companies just implementing an antivirus solution or a threat detection system and just hoping for the best are long gone, although an alarming number of firms still think this is an acceptable approach to security. Many think "it will never happen to me". Newsflash. It does.

Educating every customer on the importance of having a tight security strategy is vitally important.

These days companies really do have to plan for every eventuality, particularly if they hold sensitive customer data themselves. And often they cannot do it alone. They need guidance from the experts.

In this section, the report will examine some of the technology trends that businesses should be considering as part of their everyday security strategy.

According to a report by Dimension Data *(Source 12)* one of the trends the market is seeing is the return of a **'zero trust' security strategy**, where IT teams adopt a 'we don't trust anybody' mentality, meaning each individual user needs to pass strict authentication measures that verify their identities through multiple credentials, also known as **multi-factor authentication.**

This means more firms will turn to their security providers to help them achieve this goal and keep their strategy current and secure. And while it may seem a pain to their employees who would naturally just prefer a simple password mechanism, it is a good way to eliminate some of the more basic threats.

Dimension Data also predicts a rise of **deception technologies** being deployed this year, which works to combat the risk posed by IoT adoption, by introducing thousands of fake credentials onto an organisation's network, making it near impossible for a cybercriminal to find the legitimate information. But once the fraudster tries to use a fake credential, the security team are alerted to their presence and take steps to stop them.

The rise of **Artificial Intelligence** (AI), is also a trend that is impacting security. More and more vendors are jumping onto the AI bandwagon and building 'smart' systems that can detect and act on security threats, either before or soon after a breach.

This is augmented by machine learning or 'deep learning' capabilities and advanced analytics technology that can make computers and systems more aware of threats, more intuitive and importantly more defensive without human intervention. There is even an increasing army of automated 'threat seekers' - fuelled

by AI technology - being deployed in the corporate world that actively track down and hunt the fraudsters before they can take action.

However, there is always a reverse threat with AI, because the hackers can also find ways to manipulate the technology so it works in their favour.

Blockchain is also a technology that can be used in the fight against cybercriminals, Dimension Data predicts. Because the technology allows a 'digital ledger' of transactions to be created and shared among users on a distributed network of computers; organisations could make Blockchain-driven transactions internally visible so they can see every single one that takes place. Anything suspicious can be flagged and solved quickly and cleanly.

Social Media is also a double-edged sword for many companies. While it is a fantastic way to spread the corporate word, gain followers (potential customers) and broadcast success, there is also a risk that 'leaky' apps could compromise a company's security if they fail to have a strict protocol in place.

Common risks include spreading a virus to all your followers by not monitoring the app carefully enough, careless employees accidentally sharing sensitive information and hackers gaining control and using the corporate account for phishing purposes or for spreading false information to damage a reputation. It is vital to have a proper strategy in place, and ensure employees are fully educated.

Compliance is definitely an area that cannot be ignored. Despite all the hype surrounding the General Data Protection Regulation (GDPR) that came into force in May 2018, companies must comply with these laws or they could end up facing a crippling fine.

Another crucial area that firms must be up-to-date with is **disaster recovery (DR)**. That way, if their systems and data are ever compromised by an attack, they can easily revert to a point before the attack took place and carry on business as usual. One thing all companies cannot afford in this fast-paced world, is downtime.

While this may seem like a very basic and obvious requisite, **email security** is a must have for today's corporates – many companies don't even think about this as a vital line of defence, but have a properly encrypted and protected email system will stop a lot of attacks in their tracks and keep sensitive data protected.

This may also seem ridiculously simple; but ensuring all security applications are **regularly updated** will also combat some of the more basic threats. Again, this is a service often provided by the channel, but there are still many companies out there – granted, the smaller ones – that fail to realise how at risk they are by having outdated security applications on their systems.

As mentioned earlier, the amount of different technology sets and variants are far too numerous to mention, but by considering the above, at least firms will be on the right track. Which vendor technology is deployed, is another conversation entirely.

Section Five: Obstacles for Customers

Customers today are faced with a barrage of information over security and they struggle to process it, so this is where they desperately need the support of a trusted IT advisor.

Because IT and security are not part of their core business, they need to feel safe in the knowledge that they are adequately protected against all threats, but that the technology they buy into will not keep them from doing their day job and create more work and hassle.

A key part of convincing customers to investing in security is making sure they properly understand the threats that directly affect them, without resorting to scaremongering tactics.

Many are reluctant to part with their money for the sake of it, so they need to be sold to in a way that will convince them to make the investment. The only way to do this is an outcome-based sales approach and making sure explanations are kept simple, rather than overly technical (blatant plug, we know, but **Boost Training**, a division of Boost Technology Group, are specialists at helping tech companies develop effective outcome-based sales programmes, so may be able to help your team here). The saying 'Keep it Simple, Stupid' or KISS, is definitely needed when selling security.

Also, the customer buying chain has evolved, with spending decisions being taken at board level - both in enterprise and SMB customers - rather than at IT department or IT manager level. Budgets are more tightly controlled than ever. And rightly so.

If a reseller, MSP or MSSP can explain a technology strategy and the need to invest succinctly and simply to a board of directors that are not technically minded, then they are more likely to part with their cash if they realise the real risks they are facing and what failing to invest could do to their business.

The other obstacle many IT suppliers face, particularly with smaller customers or some public sector customers, is the fact that they have been burned by suppliers in the past and are reluctant to trust another IT provider with their infrastructure.

Many have been promised the earth by previous IT service providers who then delivered little or nothing promised, which has cost them time and money, and in some cases caused them to suffer a significant security breach and lose reputation with their own customers as a result. It is no wonder they are suspicious of new suppliers and need careful handling.

Section Six: Channel Challenges

Of course, the issues run both ways; with each sceptical customer comes a range of challenges for suppliers to overcome, with the added bonus of having to deal with a constant barrage of information from vendors claiming to offer the best solution on the market.

The channel is faced with pressure on all sides, but often the best strategy is not trying to be a jack-of-all-trades and master of none, but by really focusing on an area of technology that suits your customer base.

It might seem obvious, but there are plenty of partners that try to over-stretch themselves and end up lacking the resources and skills to fulfil their obligations to customers. And this is where reputations are lost.

This means working only with vendors that can offer their partners a good return and a secure strategy to invest in, it is all very well getting carried away with exciting start-up technology, but if they fail to have a proper business plan or plan of action in place for their partners and their products, it is money down the drain. Proper research is vital when selecting suppliers.

Luckily for the channel, this is where distribution comes into its own, as distributors that specialise in security will have done their due diligence on the vendors they promote, thereby giving Resellers, MSPs and MSSPs the peace of mind that they and their customers need.

Being honest with customers from the start and promising them realistic outcomes will prove more beneficial in the long run, rather than promising the moon on a stick and failing to deliver.

Patience when dealing with these customers, taking the time to get to know them and listening to their needs first, is the only way to regain their trust and convince them to place their faith in you as a supplier.

And it dœsn't end with them signing on the dotted line. Remaining proactive and keeping customers informed of any updates or changes is vitally important. Without communication customers feel neglected and unimportant. But by staying it touch, it could actually lead to additional business opportunities further down the line.

Section Seven: Conclusion - Security Should be Integrated into Everything

As this report has proved, security is an area of huge opportunity for the channel, but it is a market that needs careful research and the right approach to customers.

Security should be a part of every sale, not just an afterthought; the number and complexity of threats facing companies on a daily basis means it is not something that can be ignored or put on the back burner.

The fact is, security really isn't a standalone sale any more – for customers of all sizes investing in the cloud, or IoT, or even those looking further ahead and investing in AI and analytical technology, the need for security solutions and services to be wrapped around all of these areas is greater than ever.

There is never a better time to be involved in this market, but suppliers must make sure they know exactly what they are getting into, what their technical capabilities are, and where they could possibly team up with peers to combine skills rather than trying to do everything themselves and failing miserably.

Keeping customers happy and secure, and able to run their businesses without worrying about technology issues, should be the ultimate priority.

Defeating the cybercriminals will continue to be an ongoing and evolving battle, which requires a multi-pronged technology approach and is a continuous learning curve. All IT service providers operating in that space need to make sure they have the right technical weaponry, along with the skills and knowledge in place to keep themselves and their customers adequately protected against any threat; present and future.

Sources:

1. https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1269
2. https://www.grandviewresearch.com/industry-analysis/security-market
3. https://www.mordorintelligence.com/industry-reports/europe-cyber-security-market
4. https://www.gartner.com/newsroom/id/3836563
5. https://www.channelnomics.eu/channelnomics-eu/feature/3033791/seven-key-takeaways-from-infosec-2018
6. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
7. https://www.cso.com.au/article/632468/top-five-global-cyber-security-threats-2018/
8. https://www.gartner.com/newsroom/id/3790965
9. https://www.idc.com/getdoc.jsp?containerId=US43624018
10. https://resources.infosecinstitute.com/2018-cyber-security-predictions/#gref
11. https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/
12. https://www.dimensiondata.com/it-trends/cybersecurity-2018

Other sources/further reading:

https://blog.barkly.com/2018-cybersecurity-statistics
https://www.cso.com.au/article/632468/top-five-global-cyber-security-threats-2018/
https://www.alliedmarketresearch.com/cyber-security-market

About Boost

Boost is improving the business performance of technology companies by revolutionising the "assisted sales & marketing" experience.

Boost's services include:

- **Value Proposition Design**
- **Go To Market Design**
- **Multi-Media Content & Asset Creation**
- **Demand Generation Design & Implementation**
- **Telemarketing**
- **Sales & Marketing Consultancy** (commission/rebate plans, sales processes etc)
- **Sales Training & Enablement**
- **Salespeople-as-a-Service – our people, trading as yours**

To learn how Boost can help you improve your business performance, contact us today.

020 3740 4074
contactme@boost-performance.co.uk
www.boost-performance.co.uk

Join the revolution.

JOIN THE REVOLUTION.

BOOST
TECHNOLOGY GROUP

Boost Technology Group
26 Dover Street, London W1S 4LY

020 3740 4074
contactme@boost-performance.co.uk
www.boost-performance.co.uk