How do you protect your small business from growing security threats?

There’s no doubt that the importance of cyber-security is growing in every type of business.

As businesses try to digitally transform themselves, security is one of the key aspects that will need to be considered. A legacy IT environment is bound to have many vulnerabilities because of the need to constantly patch and update outdated software, issues with integration and difficulties in effectively managing an entire IT infrastructure from a security perspective.

However, on the flipside, digital transformation does not mean that a business is completely secure. New types of sophisticated attacks are continually arriving, making the challenge for businesses harder. In fact, analyst firm Gartner predicts[1] that by 2020, 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.

[1] https://www.gartner.com/newsroom/id/3337617

“Digital business moves at a faster pace than traditional business, and traditional security approaches designed for maximum control will no longer work in the new era of digital innovation”

Gartner

“Digital business moves at a faster pace than traditional business, and traditional security approaches designed for maximum control will no longer work in the new era of digital innovation,” said Gartner at the time.

In essence, a digital business could be faced with a much bigger security challenges than the archaic and legacy businesses of old. However, if companies decide not to go digital, they’re effectively rendering themselves as obsolete, and so there is no hiding for companies that want to continue to be competitive.

This issue is even more prominent for small to medium businesses (SMBs).

As they’re advised to step-up and become digital to remain relevant with customers and partners, these resource-restricted businesses can be impacted more heavily than large enterprises, in the sense that they may not be able to recover at all; the US National Cyber Security Alliance found[2] that 60 percent of small companies are unable to sustain their businesses over six months after a cyber-attack.

And with the EU’s General Data Protection Regulation (GDPR) just around the corner, this threat becomes very real with potential fines for non-compliance and data breaches going up as high as €20 million (or 4% of global annual turnover).

In this whitepaper, we investigate the threat facing SMBs, what solutions they need to put in place and how Dell can support them with their security needs.

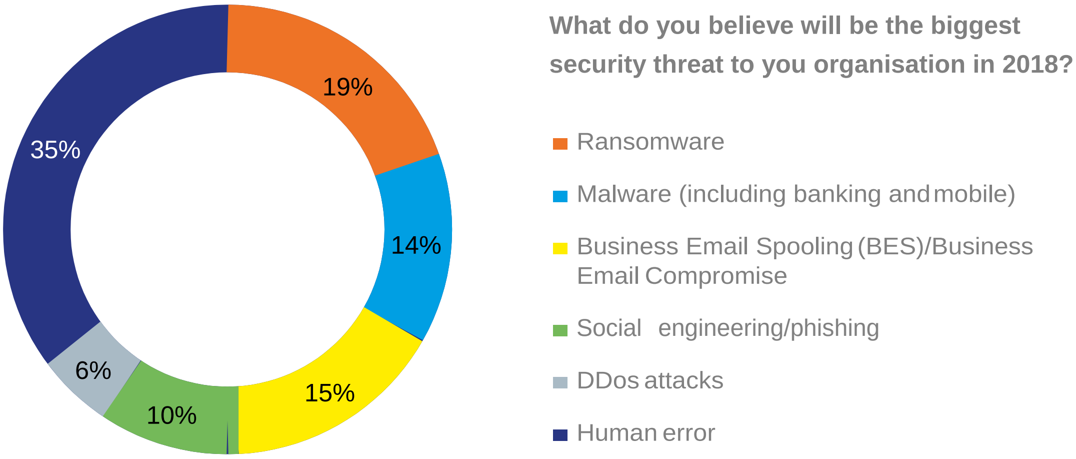
What are the latest threats facing SMBs?

The Cyber Threat to UK Businesses report[3], published by the National Cyber Security Centre and the National Crime Agency found that the cyber-security threat was “bigger than ever”, with criminals carrying out more online attacks than in the past.

The report details some of the biggest cyber-attacks in the last year – particularly the WannaCry ransomware attack[4], and the Equifax data breach[5]. However, many SMBs may mistakenly think that these security breaches are relevant for large enterprises and do not affect smaller businesses. But the report makes clear that cyber-attacks have resulted in financial losses to businesses of all sizes.

[2] https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html
[3] https://www.ncsc.gov.uk/cyberthreat
[4] https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[5] http://www.bbc.co.uk/news/technology-41737241

Over a third of IT Decision Makers believe that human error will be the biggest security threat to their organisation


What do you believe will be the biggest security threat to you organisation in 2018?

> **"The examples we've included demonstrate that small businesses are just as much at risk as larger ones"**
>
> *National Cyber Security Center*

"The examples we've included demonstrate that small businesses are just as much at risk as larger ones," the report states.

"The costs arise from the attack itself, the remediation and repairing reputational damage by regaining public trust. Attacks have also triggered declines in share prices and the sacking of senior and technical staff held to account for massive data breaches," it adds.

And it is here where it is critical that businesses, both big and small, know where their biggest vulnerabilities. For most SMBs, it appears their security problems start with a well-known problem –human error.

When IT decision makers from small businesses were asked in a recent Dell Small Business, Intel and Techworld survey[6] to select the biggest security threat facing their organisation in 2018, human error came through loud and clear as the root of all their security problems.

Approximately 35% said that 'staff accidentally or intentionally putting themselves and the company at risk' was their biggest security threat, with ransomware (19%) and business email spoofing (16%) making up the top three.

Interestingly, when it came to their biggest challenges around security, a considerable 53% (second only to human error) cited the 'pace of change in cyber-security and the evolving capabilities of threat actors' – a sure sign that many SMBs simply do not have the budget or resources to protect themselves from the threats they are now facing. Managing third-party suppliers (33%) rounded out the top three security challenges, although small business leaders did also have concerns around network visibility (25%), a lack of human resources (20%) and cloud security (20%).

The statistics on human error are perhaps not overly surprising – they mirror a 2016 Ponemon Institute survey[7] which found 56 percent of organisations reported data breaches at the hands of employees who were leaving the company or new employees, as well as a 2017 study from Kaspersky Lab[8] which found that employee carelessness accounted for 46 percent of breaches in the past year.

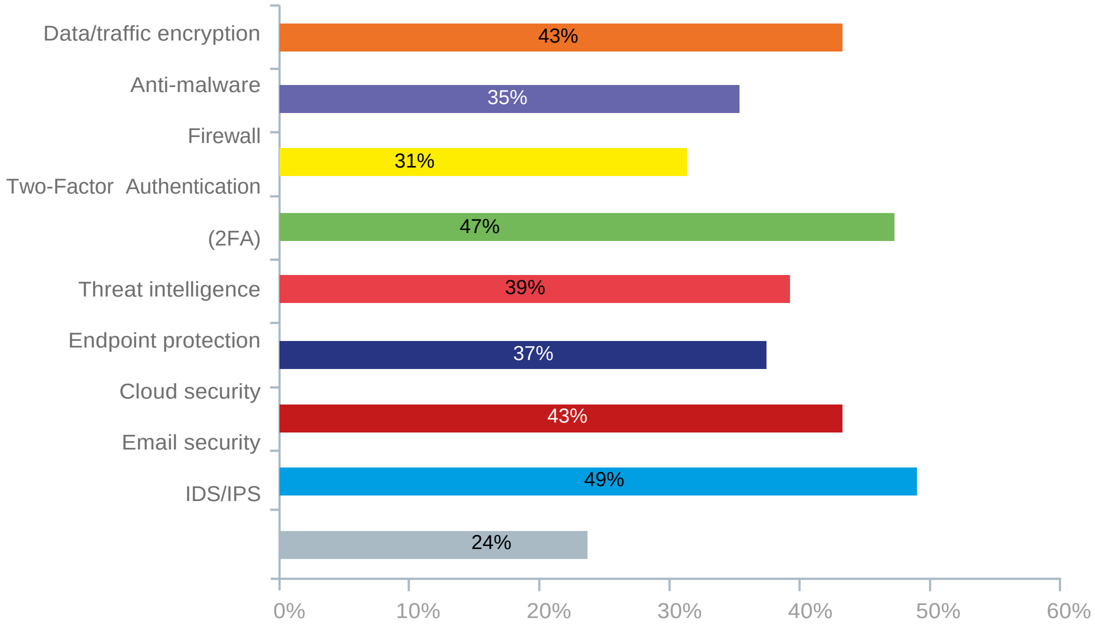
[6] Dell/Techworld research study, Evolving small business through trusted partners and technologies, 54 respondents, March 2018

[7] https://dtexsystems.com/cost-of-insider-threat/

[8] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

There are a number of technologies that organisations are looking to invest in to improve their security and thwart cyber attacks

What technologies are you looking to actively invest in to improve your security maturity?



So how do small and medium-sized businesses get themselves in a position where they can prevent such intrusions?

Analysts at Gartner[9] suggest that today's security era is as much about response as detection, so it's important to develop the appropriate internal processes, and prepare your people, so you can proactively respond to security incidents.

"Your business must be prepared – an intrusion is inevitable for many organisations and preventative security measures will eventually fail," says Rob McMillan, research director, Gartner. "The question you must accept isn't whether security incidents will occur, but rather how quickly they can be identified and resolved."

Technologies that can help small businesses

With human error in mind, it is perhaps unsurprising that much of the investment is pouring into technologies that can greatly reduce the threat.

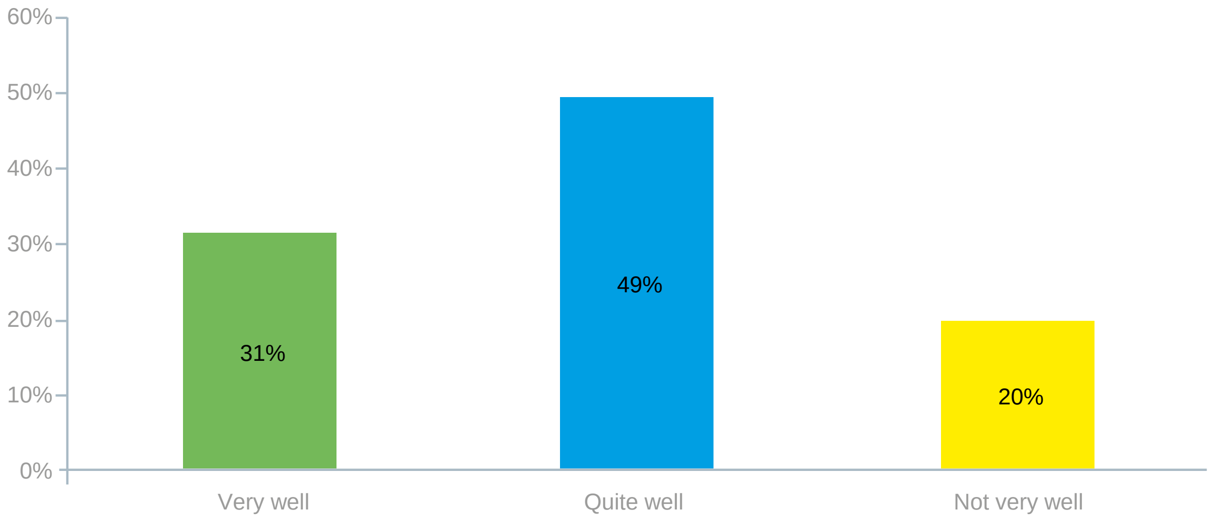
In the Dell Small Business Survey, email security (49%) and two-factor authentication (47%) ranked highest for respondents asked, 'what technologies are you looking to actively invest in to improve your security maturity?'. Data traffic/encryption (43%) and cloud security (43%) also scored highly, with the latter perhaps evidence of cloud platform providers embedding greater security and data protection controls in their public cloud options.

Yet while human error continues to be at the front face of attacks, a problem that gets attention is that these organisations don't have the appropriate tools or resources comb through their network for attacks.

[9] https://www.gartner.com/smarterwithgartner/prepare-for-the-inevitable-security-incident/

Management are starting to gain a better understanding on the cybersecurity challenges that organisations will face in the future

How well do you feel your management understand the cybersecurity challenges that your organisation will face in the future?



“Your business must be prepared – an intrusion is inevitable for many organisations and preventative security measures will eventually fail,”

Rob McMillan, research director, Gartner.

After all, a previous study from FireEye revealed that most attacks stay undetected for 175 days[10] and that is a worry with the EU’s GDPR around the corner, promising fines of up to €20 million (or 4% of global turnover – whichever is higher) in the event of a data breach.

This lack of threat detection capability, visibility into the network and ability to monitor the latest threats signal that small businesses should be investing in security monitoring and threat detection tools. Indeed, Gartner has previously cited managed detection and response (MDR) as the perfect type of solution for SMBs because it improves threat detection, incident response and continuous-monitoring capabilities for organisations that don’t have the expertise or resources to do it on their own.

“Demand from the small or midsize business (SMB) and small-enterprise space has been particularly strong, as MDR services hit a ‘sweet spot’ with these organisations, due to their lack of investment in threat detection capabilities,” Gartner said in its Top Technologies for Security in 2017[11] report.

However, surprisingly, in the Dell Small Business survey, intrusion detection and prevention systems (24%) ranked bottom out of all the technologies IT leaders are looking to actively invest in to improve their security maturity, with threat intelligence only fifth on the priorities list (39%).

Evidently, there is still some way to go before SMBs have the tools required to keep themselves protected but perhaps that will soon change, especially as SMB business leaders appear to be improving their security awareness. In the Dell Small Business survey, almost a third (31%) said their management had an excellent understanding of the company’s security challenges, with almost half (49%) saying that their management understood these challenges ‘quite well’. Only 20% said that managers didn’t have a good understanding of their security challenges.

[10] https://www.computerweekly.com/news/252438158/Average-attacker-dwell-time-nearly-six-months-for-EMEA-study-shows

[11] https://www.gartner.com/smarterwithgartner/gartner-top-technologies-for-security-in-2017/

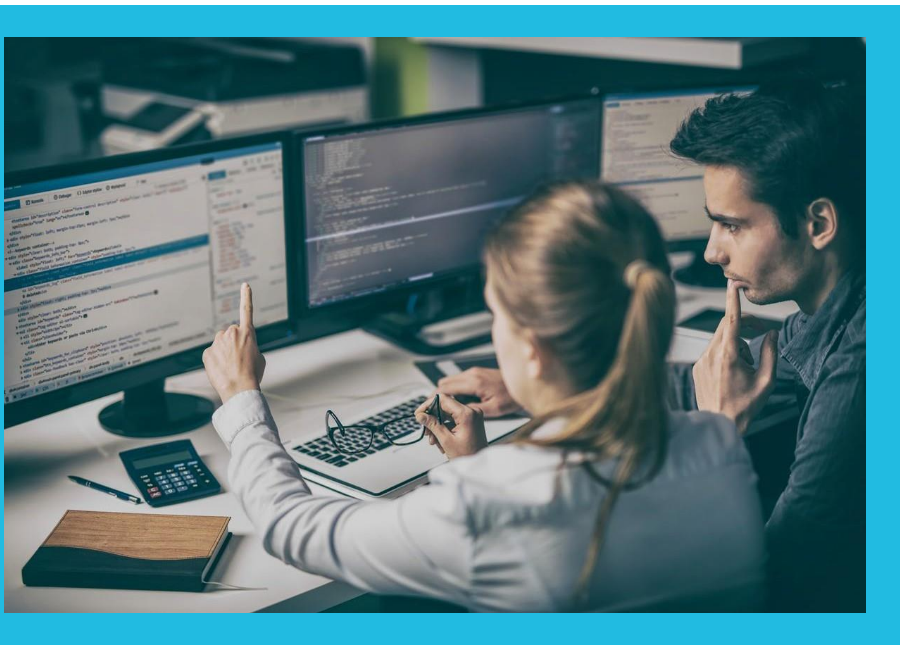
Yet it is important to note that implementing new technology is not the only way to improve IT security. Gartner suggests that the top priority is focusing efforts on patching vulnerabilities that are being exploited in the wild or have competent compensating controls that can. It says this is an effective approach to risk mitigation and prevention and yet very few organisations do this.

Preparing for GDPR

As the incoming EU General Data Protection Regulation come into force, organisations will be pushed to ensure that the way they are prepared for the new rules or pay the consequences. As the law affects anyone holding data on EU citizens, including those companies not in Europe, many smaller businesses will be affected.

As digital enterprises are relying more increasingly on data to gain a competitive edge, it is particularly important that small businesses pay attention to how that data is safeguarded. This starts from how they obtain data – as they will now often need separate user consent to use customer data for different things such as marketing and support.

> **“The question you must accept isn’t whether security incidents will occur, but rather how quickly they can be identified and resolved.”**
>
> *Rob McMillan, research director, Gartner.*



Furthermore, they need the ability to delete that data if a customer withdraws consent, and the ability to provide a machine-readable copy of the data so that a customer can send it to another provider if they wish to do so. These can both pose challenges for small businesses because they may not have a formal structure for handling data in place, and because a small business is more likely to rely on third-party data handling services, making them data processors (and not data controllers). This means they need to ensure their contracts with service providers are clarified, to ensure data can simply be erased or ported, and the process of doing so.

Businesses may need external support to help with data governance obligations that make-up part of GDPR, while they will need someone in-house managing security policies and procedures. GDPR isn’t merely a tick-box exercise, companies will continually have to adapt and ensure they are compliant with the legislation.

Finally, data breach notification becomes mandatory under the GDPR, even for small businesses. If an enterprise fails to notify the data watchdog in their region they could face huge penalties that can be crippling for small organisations, even potentially putting some of them out of business.

How can Dell help?

Small businesses are focused on efficiency and scalability, retaining and attracting the best talent and ensuring that their platforms are both easy to use and secure. However, driving innovation and reliability at the same time is no easy task, especially as many of these variables are ever-changing. This is why small firms are largely looking to technology and technology providers to help them with these challenges, and to drive innovation; in a recent study by IDC[12], two thirds of UK SMEs said they were using technology to improve their business to keep up with digital transformation.

In the Dell Small Business survey, data security was cited as one of the coming year's highest priorities for nearly half (49%) of IT decision makers with 10% saying it was the highest priority.

Dell offers comprehensive encryption, advanced authentication and leading-edge malware prevention from a single source, ensuring small businesses get robust, centralised data security, and protection from data security breaches, with the highest level FIPS certification.

As the Dell Small Business survey showed a range of security concerns, and a number of different data points that needed to be secure including the cloud – Dell Data Protection/ Encryption protects data on devices, as well as external media, self-encrypting drives and in public cloud storage all from a single solution suite, so our users get a secure network from every touchpoint.

Meanwhile, Dell Small Business Technology Advisors give businesses the technology, advice and one-on-one partnership required to fuel business growth. Dell works with its partners to understand their needs and provide them with the right solutions for success.

Today's small business owners can have dedicated resources and tailored solutions to be successful in their markets – from selecting the right systems, to incorporating servers or creating networks, and making sure all of these are secure.

But the partnership is more than just about picking the right technology. Dell's highly-trained advisors can help ensure that the technology performs the way it needs to, even as the business evolves. This means, when it comes to reliability and security, Dell's advisors can ensure that any small business has the right tools in place, adhering to regulations and best practice – particularly when changes are made, or new security threats need to be addressed.

Dell's job is to make it simpler for small businesses to thrive and to focus on gaining their own competitive edge, so we provide support 24/7 to ensure managing technology is easy.

By combining the ongoing support and know-how of Dell Small Business Technology Advisors and the best-in-class of Dell's security solutions, businesses can rest assured that they are as secure and compliant as possible, and work on the areas of the business that they're experts in to make a difference.

Dell.com.au/SmallBusiness

To learn more, or to speak directly to a Dell Small Business Advisor on how Dell can help secure your business, visit Dell.com.au/SmallBusiness or call 1800-812-392 or Click to Chat.

[12] ttp://smallbusiness.co.uk/uk-smes-investing-tech-growth-2535098/