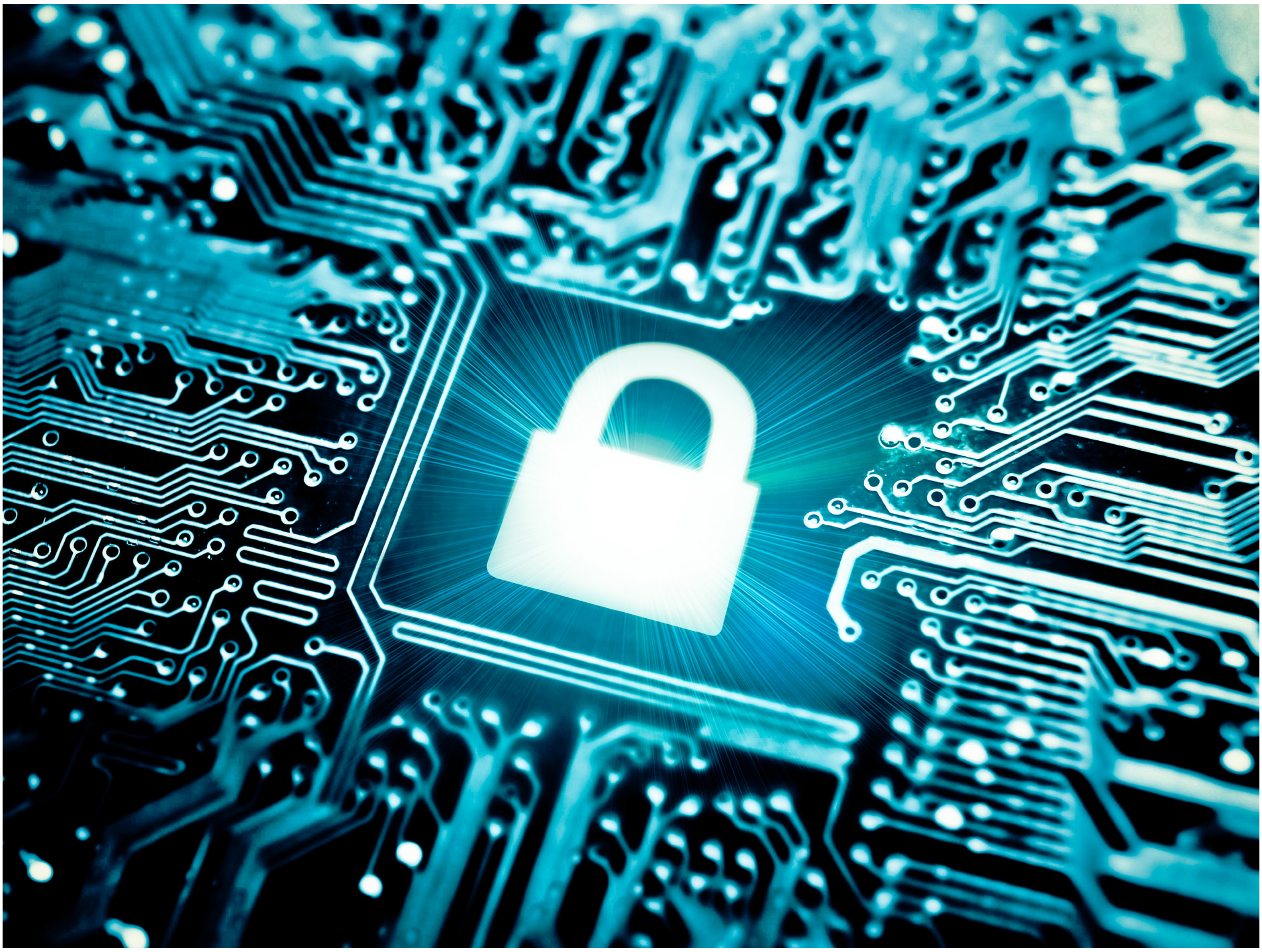


2017 SURVEY RESULTS

CYBERSECURITY: CAN OVERCONFIDENCE LEAD TO AN EXTINCTION EVENT?

A SolarWinds® MSP Report on Cybersecurity
Readiness for UK and US Businesses

solarwinds msp

EXECUTIVE SUMMARY

In this 2017 security survey, the overall responses strongly suggest that executive boards of enterprises and small to medium-size businesses (SMBs) are confident of their cyberthreat preparedness, low vulnerability, and data protection. The data reflects that their CIOs, heads of IT, and even their CISOs are all equally clear: we are secure.

This conviction has become so important to organizations that, as more high-profile hacks and breaches are revealed, often resulting in brands taking a financial or reputational hit, budgets to maintain their supposed security are being continually ramped up. Indeed, more investment is being made every year in corporate cybersecurity just to maintain that level of confidence.

Survey results suggest that IT providers are confident of their cyberthreat preparedness–but is this confidence misplaced?

Our survey reveals that it is, in fact, misplaced.

ABOUT THIS SURVEY

In early 2017, SolarWinds MSP investigated the cybersecurity preparedness, experiences, and failings of 400 SMBs and enterprises, split equally across the UK and the US.

While 87% of organizations have complete trust in their security techniques and technology—and 59% believe they are less vulnerable than they were 12 months previously—71% of those same organizations have been breached in the past 12 months. The belief that "it will never happen to us" simply doesn't hold true.

So, why is this disconnect occurring? Simply put, companies are overlooking seven basic security principles:

1. Security policies are inconsistently applied.
2. User training is massively under-prioritized.
3. Only basic technologies are being deployed.
4. Vulnerability reporting is often weak, or even nonexistent.
5. The majority of organizations make no changes to their technology or processes following a breach.
6. Widely accepted prevention techniques and processes remain overlooked.
7. Detection, response, and resolution times are all growing.

Companies looking to maintain or improve their security must pay attention to these key principles, or their overconfidence can lead to an extinction event for their business.

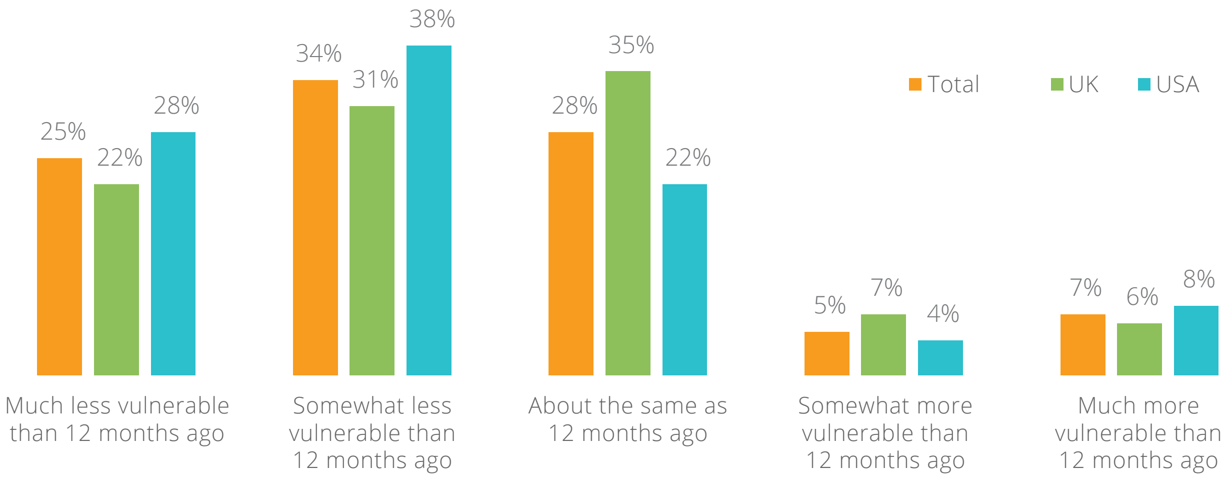
CONTENTS

IT HEADS ARE OVERCONFIDENT IN THEIR CYBERSECURITY READINESS

At first sight, perhaps the IT heads in US and UK businesses are right to be confident. The vast majority, 87%, believe that their organization's implementation of security techniques and technology warrants a rating of "average" or better. And given that 61% are about to receive a substantial boost to their cybersecurity budgets, they are confident that this position will improve.

Last year, the "IT Security Survey" by SolarWinds, which targeted the same type of companies as the current report, found that 50% of respondents believed that their organization was less vulnerable in 2016 than in the previous 12 months. This figure has now risen to 59%.

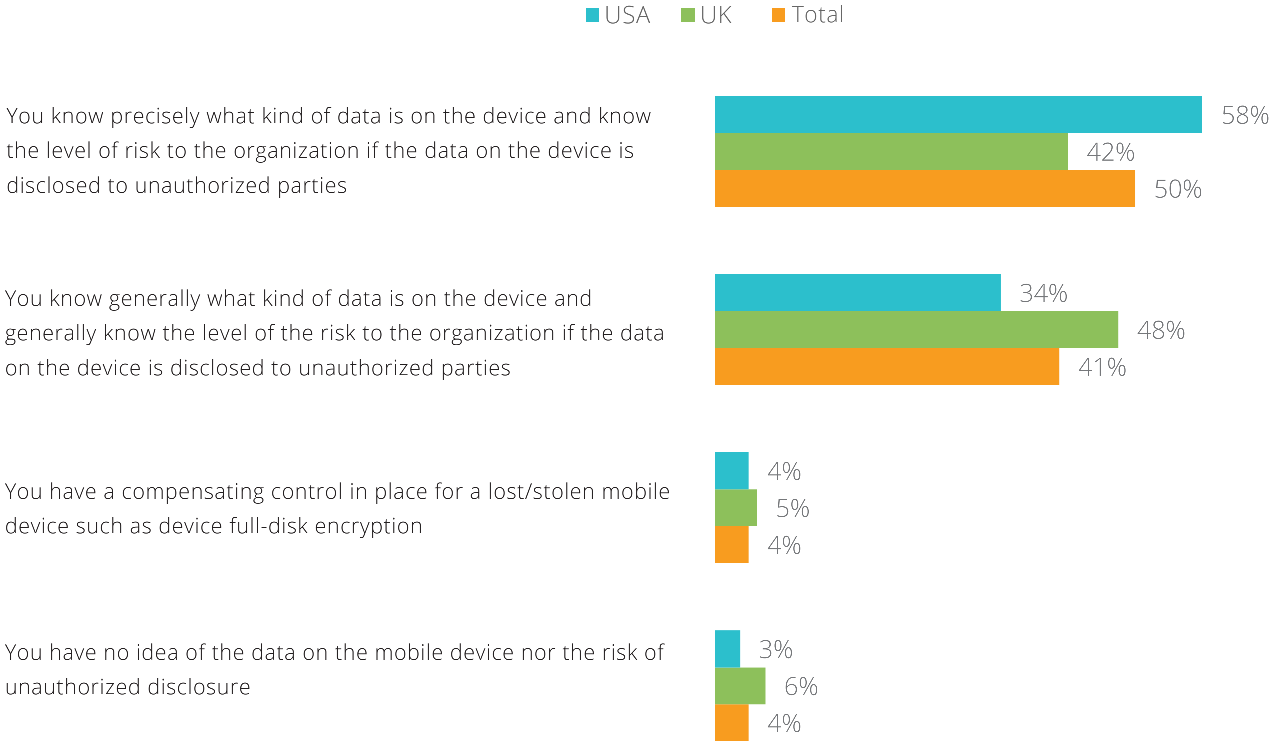
How would you describe your organization's vulnerability?



87% believe their security implementation is average or above

And it is not just “high level” self-assurance. They also have confidence in their ability to tackle very specific threats and requirements. For instance, 50% are certain that should a mobile device be stolen, they would know exactly what data was on it and the level of risk to the business. And despite the recent and notable growth in data loss and breaches, 57% are sure of the measures they have in place to protect clients’ and employees’ personally identifiable information (PII).

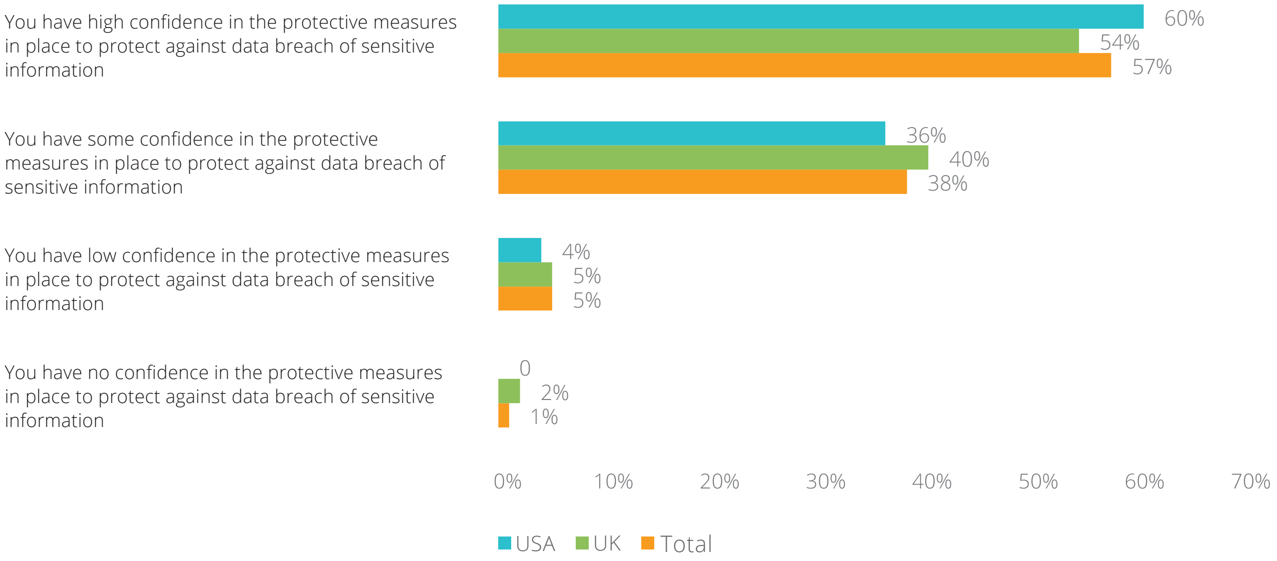
In the scenario that a human resources or operations manager/director/vice president has lost or had a mobile device stolen, which of the following is true?



Less than 50% of businesses implemented new security technologies after a data breach

14% did nothing at all

Considering the importance of all personally identifiable information (PII) held by the business on clients and employees, which of the following best describes you?



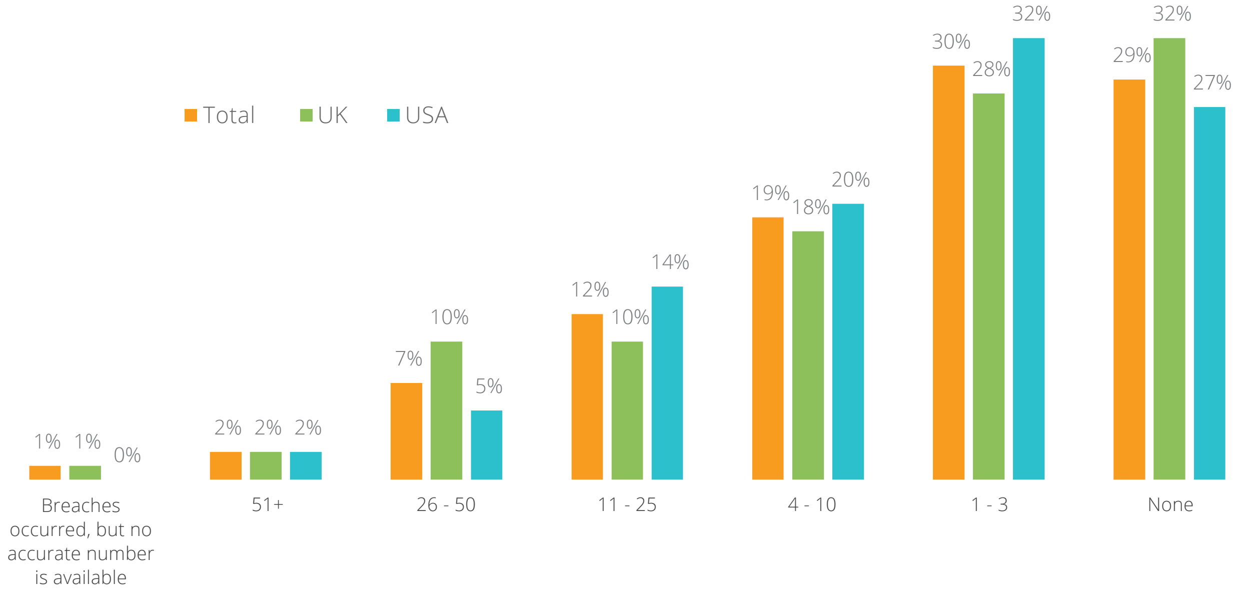
57%

of IT heads have strong faith but as our data shows, it may be misplaced

THE REALITY

The great irony is that while 87% consider themselves to have implemented average or better cybersecurity defenses and feel they're less vulnerable than they were 12 months ago, 71% reported at least one breach in the last year. This is compared to only 29% reporting a breach in the 2016 report.

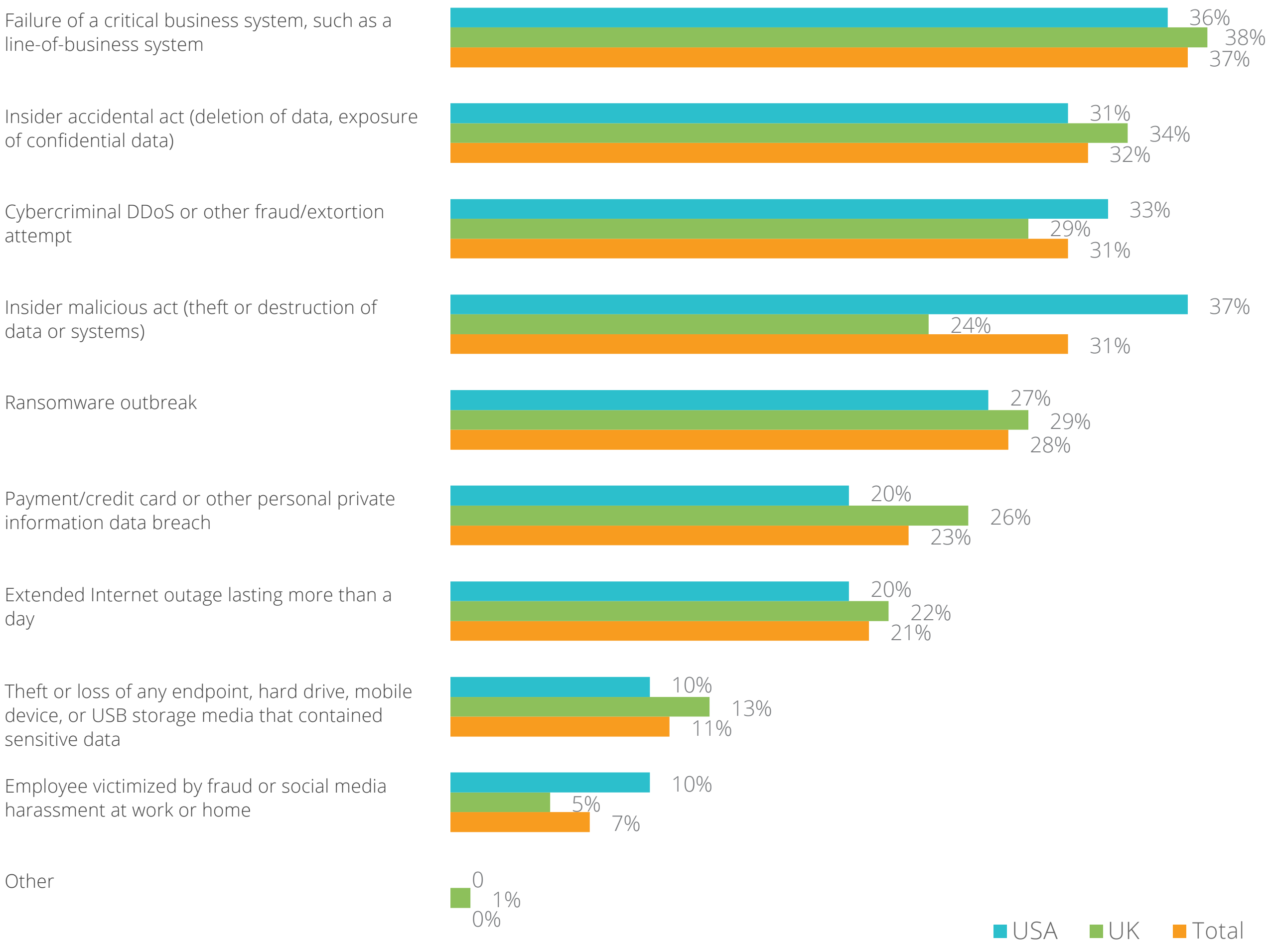
How many security breaches did your organization experience in the last 12 months?



71%

of respondents reported at least one breach in the past year

What types of security breaches have you suffered in the past 12 months?
(of the 283 who reported a breach in the past 12 months)



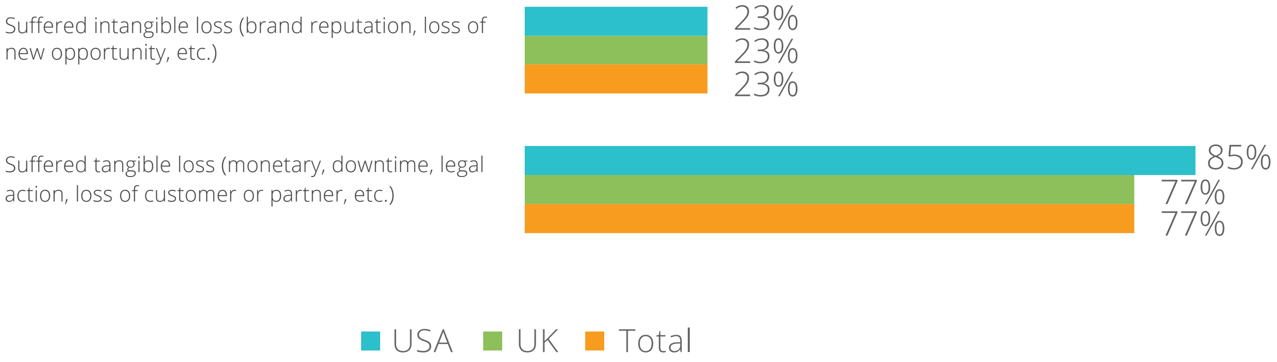
Distributed Denial of Service (DDoS) attacks, fraud and malicious insider acts account for nearly one-third or 31% of breaches

THE IMPACT

The impact of these breaches is significant.

Just 13% of the respondents who had been breached could identify an immediately traceable impact. In some cases, this was a tangible loss, such as the loss of a customer or partner, financial loss or operational impact such as downtime. Others suffered intangible losses, such as brand reputation damage or a lost opportunity.

Examining your last security incident, what best describes your organization? (of the 52 respondents who could identify a traceable loss)



77% of respondents reported tangible loss (monetary, legal action, loss of customer) from a security incident

23% of survey respondents reported intangible loss (of brand reputation, etc)

So, in hard commercial terms, what does this vulnerability cost a typical SMB or enterprise? Beyond the readily identifiable impacts of a lost customer or downtime leading to lost opportunity, what are the wider implications?

In their "2016 Cost of Data Breach Study: Global Analysis," [1] IBM and Ponemon calculated a standard cost per lost or stolen record of USD $158/ GBP £122. This calculation included direct expenses (e.g. engaging forensic experts, outsourcing hotline support, and customer relationship remedial costs such as discounts on products and services) and indirect costs (in-house investigations and internal communications). It also extrapolated typical values of lost customers and the impact of brand damage on future customer acquisition.

Combining this metric with our own data, we can see that the impact to SMBs and enterprises is extraordinary:

	SMB	Enterprise
Average number of records* held	482	5,946
Average cost per lost/stolen record* (IBM/Ponemon)	GBP £122 USD $158	GBP £122 USD $158
Typical cost of a single data breach to a generic SMB/Enterprise	GBP £58,703 USD $76,214	GBP £723,596 USD $939,444
Average number of breaches suffered in 12 months	0.32	1.05
Typical yearly cost of data breaches to a generic SMB/Enterprise	GBP £18,844 USD $24,465	GBP £757,251 USD $983,139

*A record is defined as a piece of information or data field that is linked with one or more pieces of information or data fields containing PII.

No company can afford this degree of liability, so we took a closer look at assessing why this vulnerability exists. We found seven common factors that shed insight into this misplaced confidence.

[1] Source: https://securityintelligence.com/media/2016-cost-data-breach-study/

THE SEVEN PITFALLS OF CYBERSECURITY

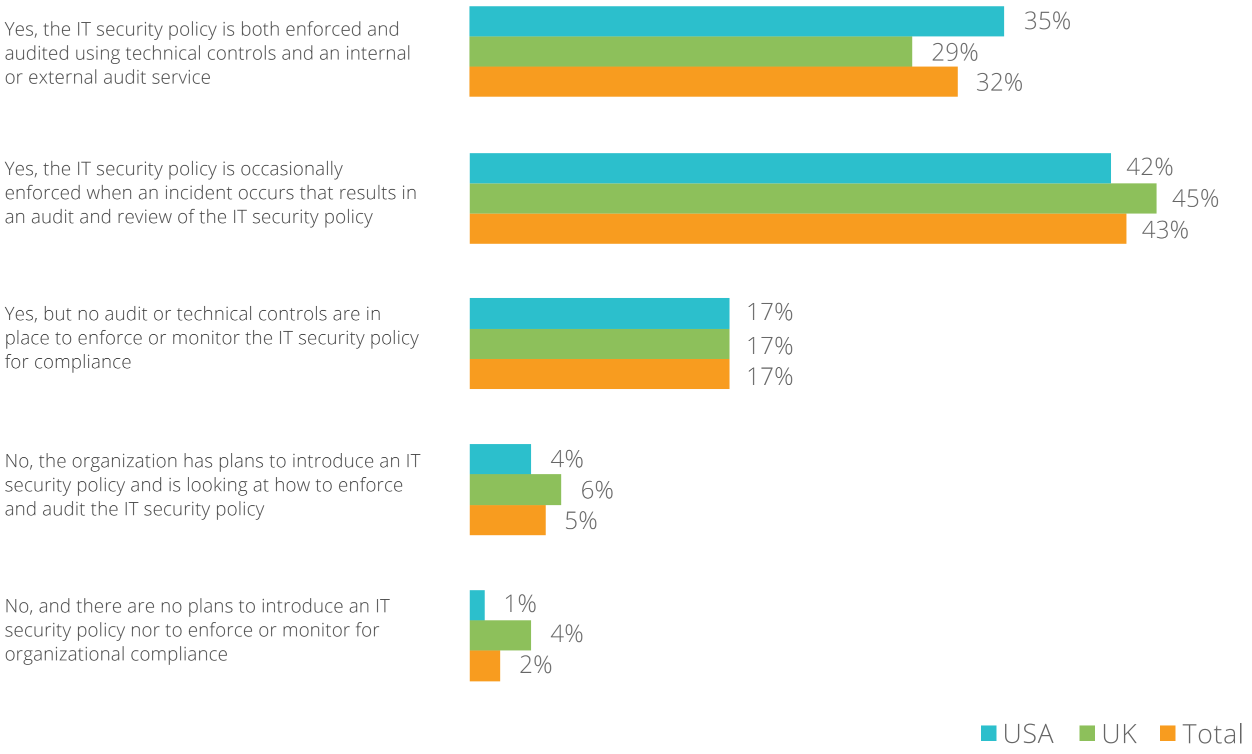
Based directly on our research, the following represent the top seven pitfalls that are opening UK and US businesses up to massive financial liabilities, with the potential for something as serious as an extinction event.

1. INCONSISTENCY

IN ENFORCING SECURITY POLICIES

A security policy is clearly worthless unless it is correctly enforced and its suitability is regularly checked. However, only 32% of respondents could claim their security policies are reliably applied and regularly audited. On top of this, less than half or 43% enforce them only occasionally, 17% fail to audit their suitability, and 7% have no policies in place.

Does your organization have an IT security policy that addresses the use, creation, and processing of employee and customer information?



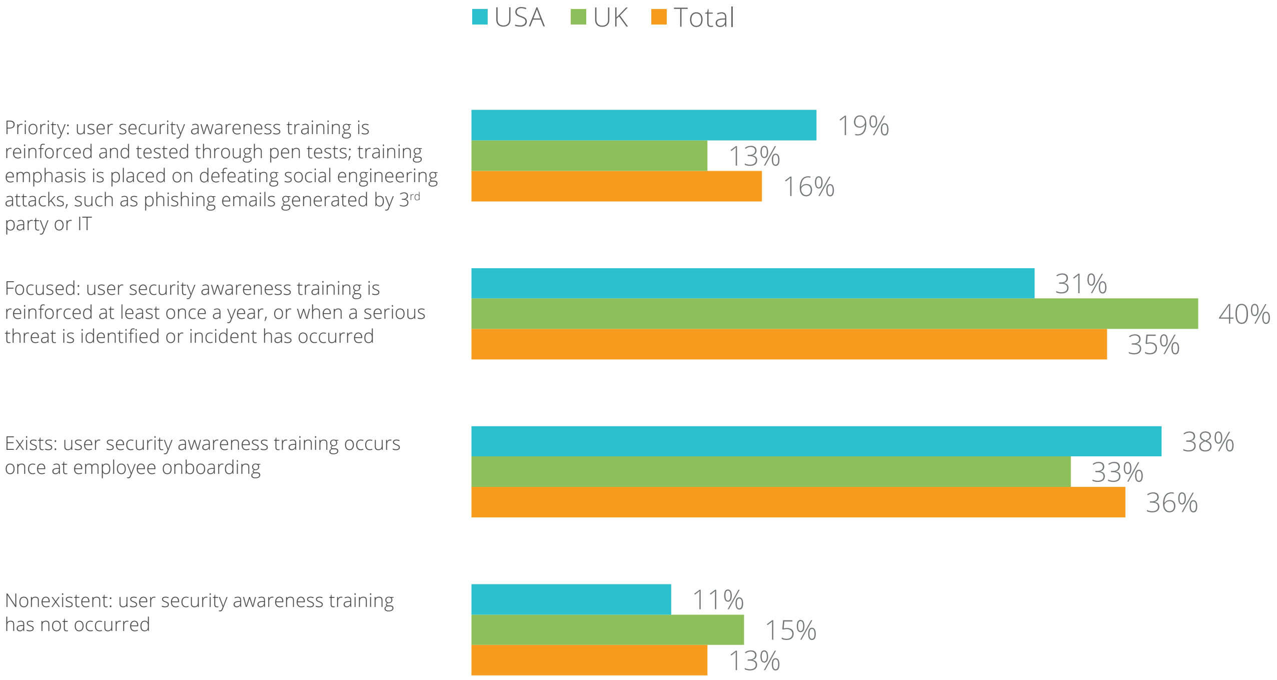
68% of respondents don’t reliably apply or audit security policies

2. NEGLIGENCE

IN THE APPROACH TO USER SECURITY AWARENESS TRAINING

Despite all the commentary about its importance, only 16% of respondents considered user security awareness training a priority. A massive 71% pay lip service to it by either including security awareness as a one-off event at employee onboarding or reinforcing it once a year. The remainder, 13%, admitted they do nothing.

Considering the users of your organization, how would you describe the current level of awareness training?



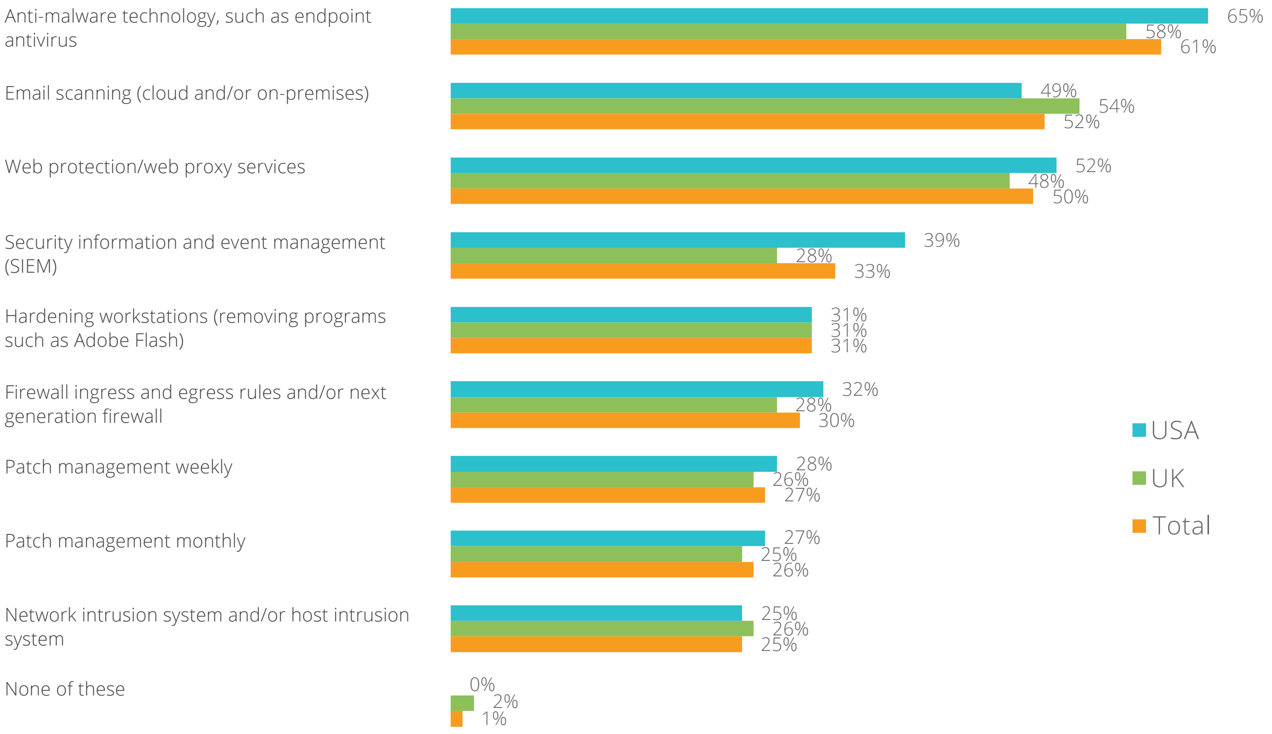
Only 16% of respondents consider user security awareness training a priority

3. SHORTSIGHTEDNESS

IN THE APPLICATION OF CYBERSECURITY TECHNOLOGIES

Six of the nine most typical cybersecurity technologies had been deployed by only a minority of respondents. Web protection, email scanning, and anti-malware had each been rolled out by 50-61%, but the remaining six (including SIEM, firewall rules, and patch management) had been deployed by only 33% at the most (SIEM), or 25% at the lowest (intrusion systems).

Which of the following technologies have you implemented on-premises to prevent data breaches?



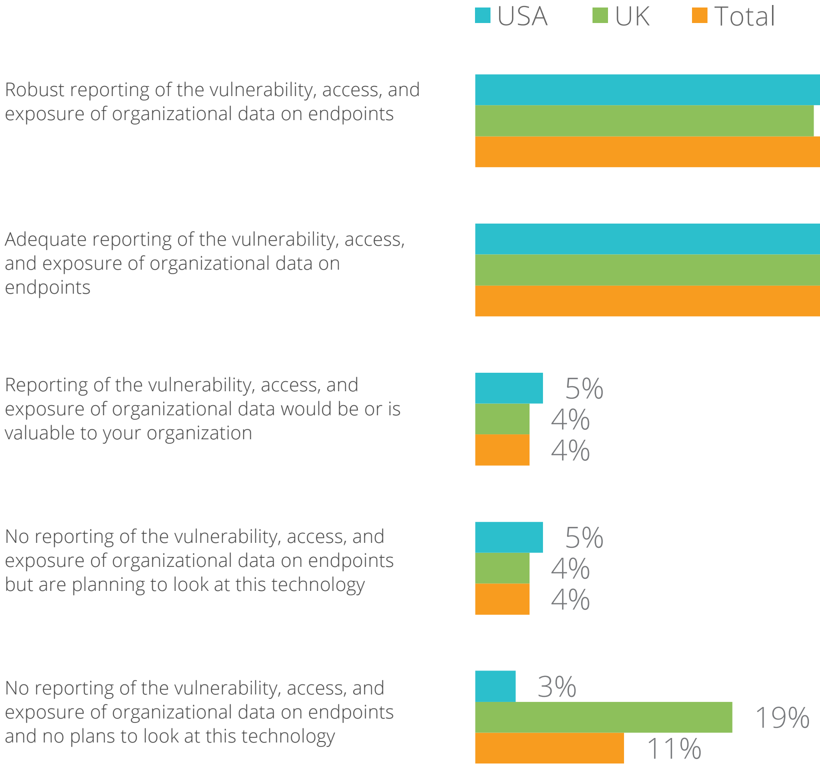
6 out of 9 top cybersecurity technologies are deployed only by a minority or less than 31%

4. COMPLACENCY

AROUND VULNERABILITY REPORTING

Only 29% of respondents could call their vulnerability reporting robust, with the majority, 51%, optimistically classifying it as adequate. Surprisingly, as many as 19% have no reporting, and 11% even said they categorically had no plans to investigate its deployment or usefulness.

Which of these reporting scenarios best describes the reporting process you have in place?



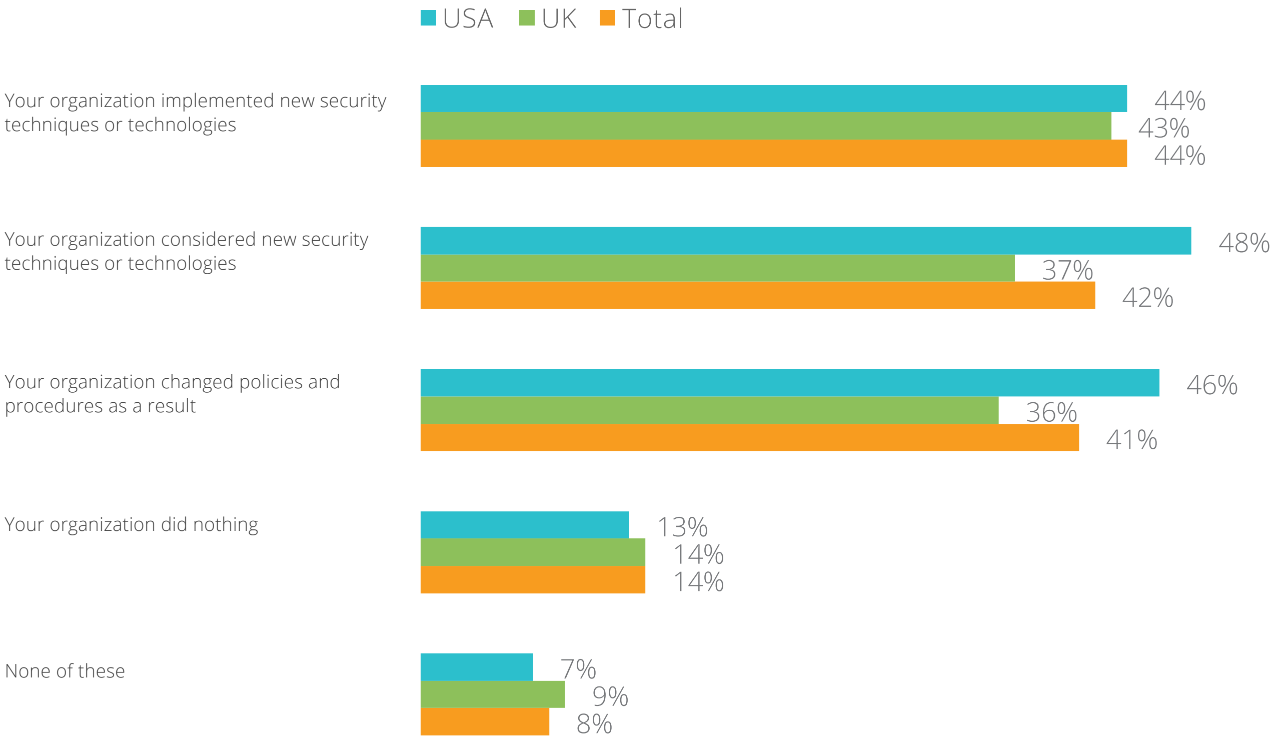
Only 29% can call their vulnerability reporting “robust”

5. INFLEXIBILITY

IN ADAPTING PROCESSES AND APPROACH AFTER A BREACH

Following a breach (experienced by 71% of respondents), only 44% implemented new technology, and only 41% changed their processes. Meanwhile, 42% started looking into new technology, while 14% purposefully did nothing.

Examining your last security incident, what best describes how your organization responded?



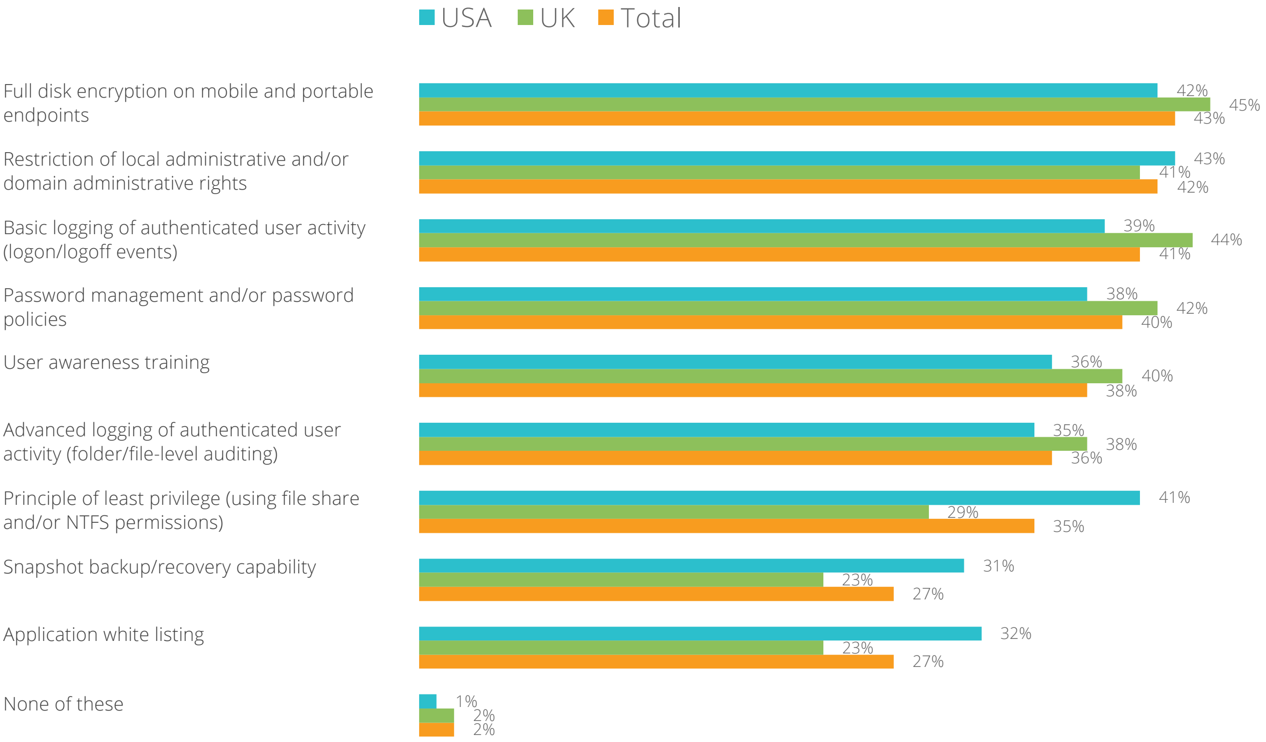
Only 44% of respondents rolled out new technology after a security breach

6. STAGNATION

IN THE APPLICATION OF KEY PREVENTION TECHNIQUES

Of the nine key prevention techniques listed, only a minority of respondents had implemented all of them. The most prevalent technique was full disk encryption on mobile and portable endpoints, but even this was only performed by 43%. Application white listing was implemented by only 38%, and logging of authenticated users' activity was used by only 41%.

Which of the following techniques have you implemented on-premises to prevent data breaches?



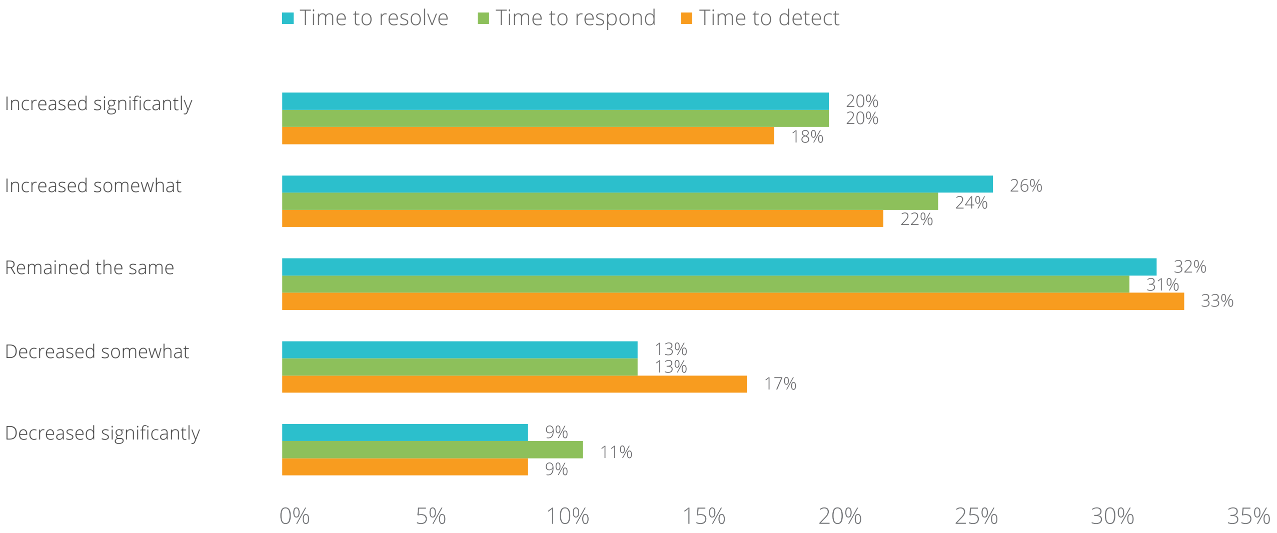
The majority of respondents failed to adopt the 9 leading prevention techniques

7. LETHARGY

AROUND DETECTION AND RESPONSE

Over the past 12 months, detection times had risen for 40% of respondents; response times were up for 44%; and resolution times had increased for 46%. In contrast, in our 2016 report, detection times had risen for only 28% of respondents; response times were up for 28%; and resolution times had increased for 27%. This shows that the rate of decay (and complacency) is growing.

Comparing 2016 to 2015, how have time to detection, response, and resolution times changed in your organization?



The survey shows that:

Detection times have grown for 40%

Response times have grown for 44%

Resolution times have grown for 46%

ADVICE FOR MSPS

The data and conclusions in this report make one crucial point overwhelmingly clear: **Enterprises and SMBs alike are overconfident in their cybersecurity preparedness.**

This being the case, what opportunities do managed services providers (MSPs) have?

Opportunity #1: Offer cybersecurity training to your customers. Training can make a huge difference in your clients' security, so it's absolutely essential that you arm them with the knowledge they need to prevent breaches. Whether you offer it as a service to build revenue or you offer it free to provide retention, training can cut down on the number of security incidents. That translates to fewer emergency calls and, ultimately, happier clients.

Opportunity #2: Make sure your own house is in order. MSPs need to make sure their own security practices are up to par. You should review your practices and security technology stack not only for current best practices, but with an eye to the future as well. Does your security meet the current and future needs of the typical SMB or enterprise? Does it work well across on-premises, cloud, and hybrid environments? Can you serve clients in highly-regulated verticals?

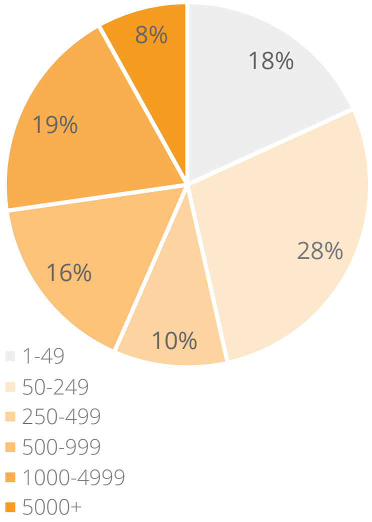
Opportunity #3: Prepare with disaster drills. MSPs can also offer to stress test their clients' security via "war games." Many industries run drills to help them deal with worst case scenarios: marketing teams practice their responses to PR crises, financial services organizations stress test their portfolios, and logistics teams plan for transportation hubs closing down unexpectedly. As an MSP, you can practice disaster events with your clients, both in terms of technology and processes, to discover weak points and make improvements. Are the lines of communication and equipment sufficiently robust? Are expectations and metrics reasonable? You're likely to find a few upsell opportunities in the process.

Opportunity #4: Determine the partnerships or skillsets you'll need. Many security incidents require specialists to handle, so make sure to prepare before you need it. Whether it's warding off DDoS attacks, protecting IoT at an architectural level, or implementing digital forensics incident response, you should either look to hire expertise in-house or partner with someone who can handle these for you. You never want to have to build new skills in the middle of a crisis.

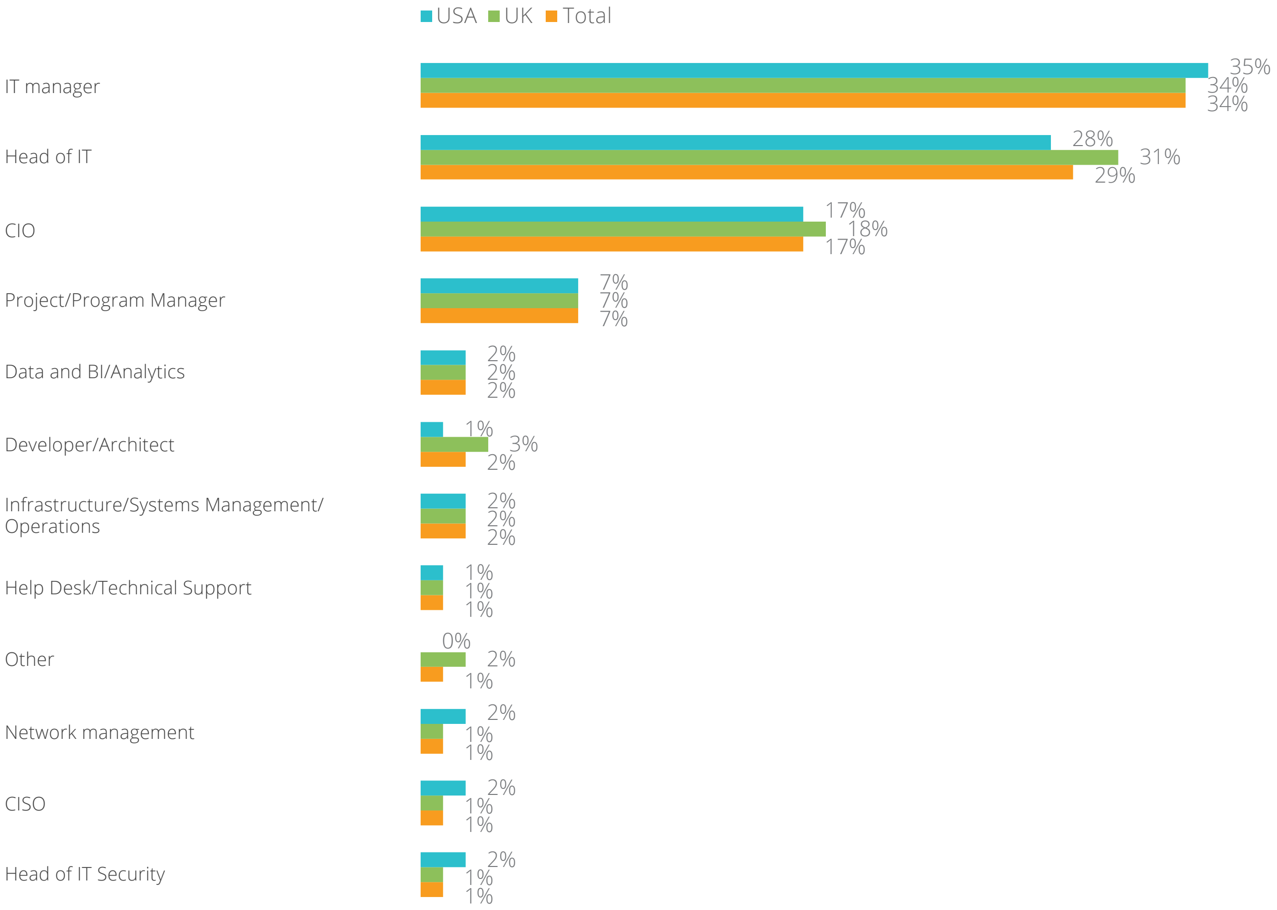
Organizations' overconfidence combined with the prevalence of the seven pitfalls of cybersecurity create a perfect storm on which cybercriminals are bound to capitalize. But with the right approach, dialogue, relationships, and tools, MSPs can turn these flaws into lucrative opportunities.

METHODOLOGY

In January 2017, SolarWinds MSP commissioned Sapio Research to investigate the cybersecurity preparedness and experiences of 401 organizations. The companies questioned were split equally across SMB and enterprise (above and below 250 employees), and between UK and US.



Employees in respondent's company	Total (401)	UK (200)	USA (201)
1 - 49	18%	22%	14%
50 - 249	28%	27%	29%
250 - 499	10%	11%	10%
500 - 999	16%	15%	16%
1000 - 4999	19%	20%	19%
5000+	8%	6%	11%



LAYERED SECURITY

COLLECTIVE INTELLIGENCE

SMART AUTOMATION

SolarWinds MSP empowers IT Providers of every size and scale worldwide to create highly efficient and profitable businesses that drive a measurable competitive advantage. Integrated solutions including automation, security, and network and service management—both on-premises and in the cloud, backed by actionable data insights, help IT Providers get the job done easier and faster. SolarWinds MSP helps IT Providers focus on what matters most—meeting their SLAs and creating a profitable business.

For more information, visit www.solarwindsmsp.com