enabling business to do business

IT SECURITY: THE EVOLVING THREAT LANDSCAPE

UNDERSTANDING THE RISKS AND MITIGATING AGAINST THE GROWING SPECTRE OF CYBERCRIME

UK RESEARCH 2016

Contents

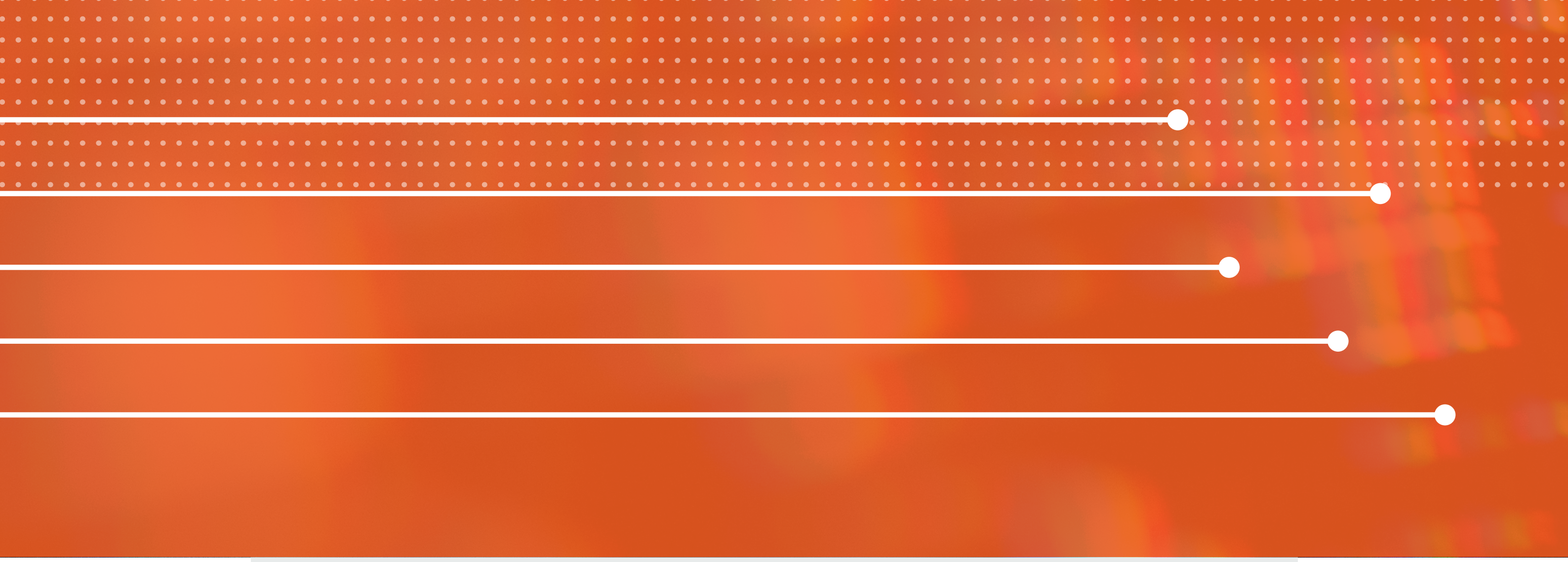
Introduction

Critical data security

Security in today’s IT environment is an ever-growing concern. As businesses become more and more connected, and operate within increasingly complex network environments, the number of attack vectors is increasing rapidly. And, as IT becomes ever more critical to the daily survival of businesses, so cybercriminals are becoming more sophisticated in their attempts to exploit vulnerabilities.

As a result, the task of securing IT infrastructures is becoming more challenging. Rarely a week goes by without news of a major, high-profile incursion into a company’s IT, (with all of the associated costs and brand damage this can bring). For many businesses, such incursions can be fatal. It is, therefore, vital that IT Decision Makers take steps to continually assess their security strategy in light of the latest best practice guidance.

This report examines the attitudes and precautions adopted by UK IT Decision Makers regarding their systems. It is written for everyone from the security professional to the non-technical manager, and is relevant to anyone who wishes to gain a view of their security preparedness or gain insight into common security practices and recommendations, that will inform and improve their own IT security strategy.



Executive summary

Complex threat landscape

Given the complex nature of both business infrastructures and the modern threat landscape, IT Decision Makers are well aware that they face an uphill struggle in trying to protect sensitive company data.

Some of the most commonly-perceived threats to businesses (the ‘human factor’) are to be expected. Others - such as a common lack of visibility into the business’ systems, a lack of ability to analyse breaches to identify cogent patterns, and a lack of knowledge of whether breaches have occurred in the first place - are both surprising and concerning.

Most ITDMs state that security is a priority, and express a degree of confidence in the precautions they have taken. However, a closer inspection reveals a number of holes in most ITDMs’ security setups. Adherence to security policies is generally poor, and the technologies ITDMs put in place do not align as well as they could with the nature of today’s typical increasingly complex infrastructures.

This paper draws on fresh research carried out among UK IT Decision Makers to explore current concerns around the threat landscape, the approaches that are in place to protect their organisations and, critically, how they can shape IT security strategies to understand and mitigate against the growing spectre of cybercrime.

Biggest security threats to a business

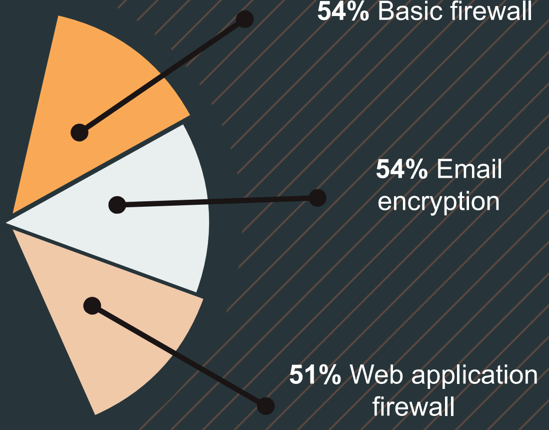
65% Human element e.g. making mistakes

48% Inability to analyse security attacks to determine cogent patterns

Where companies would spend extra budget if it became available

Security 46%

The security measures in place across UK organisations



97% of organisations have a security policy, but:

97%

52%

Only 52% say it is well adhered to by staff

12% (around one in ten) say staff do not consciously follow the security policy

Percentage of IT Decision Makers that are very confident they can handle the following:

Information leak
Very confident
23%

System compromise
Very confident
30%

Malicious attack e.g. DDoS
Very confident
27%

Research methodology

Between the 6th and 11th April 2016, independent survey company Norstat carried out an online survey of 100 UK IT Decision Makers (ITDMs). ‘IT Decision Makers’ are defined as individuals who are either ‘an influencer’, ‘one of the people responsible’, or ‘the sole decision maker’ with regards to IT systems. The respondents all worked in organisations with 50 or more employees.

NB: any inconsistencies in totalling may reflect rounding, and/or the fact that some questions are multiple choice.

Understanding the evolving threat landscape

What are the biggest threats?

Today, businesses face a plethora of threats and risks. Migration to the cloud, big data, system complexity, and a growing number of user devices, are just some of the trends that are driving an increase in the number of potential attack vectors.

The result is an increase in the volume, complexity, and intensity of attacks on businesses, with reports of high profile casualties now commonplace in today's news agenda. Yet, the threat landscape isn't one that belongs to big business; it's a critical issue for every organisation.

Security is becoming more challenging

The diversifying threat landscape, and the fact that many businesses cannot afford a dedicated internal security function, make it increasingly difficult to fully keep up with, let alone totally mitigate against, all the potential threats the business faces.

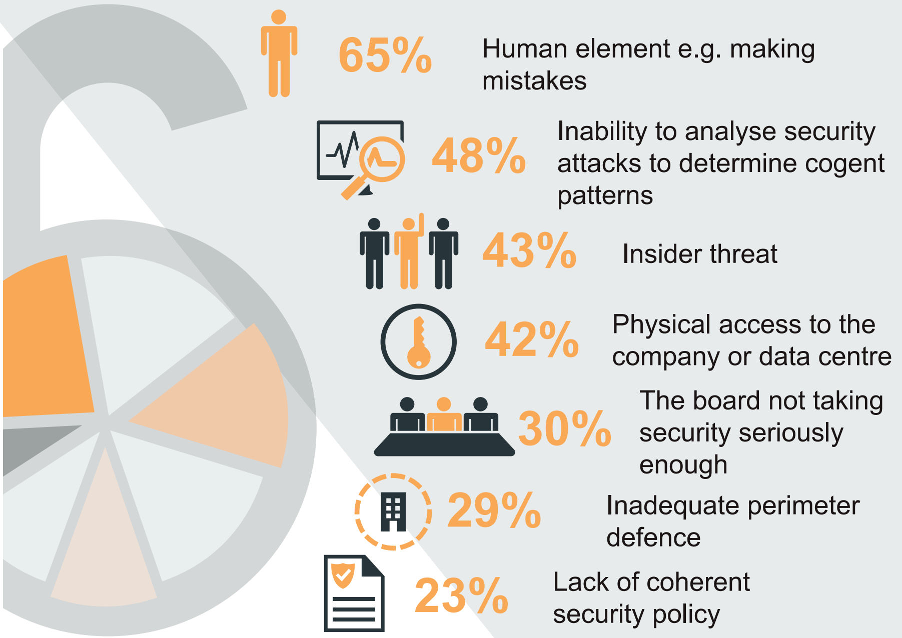
Staying abreast of, and monitoring for potential security threats is fast becoming a full-time, 24/7 job, requiring high levels of sophistication, both in terms of knowledge and the technologies used. Security professionals are expected to be both omniscient (understanding every possible threat) and omnipresent (seeing into every corner of their infrastructure). A near-impossible task.

In contrast to the 'lone wolf' security professional of old, essentially 'manning the ramparts', an increasing number of security professionals are seeing the appeal in drawing in third parties to maintain the required visibility of complex and sprawling infrastructures, and to gain access to the specialist skills required to keep track of ever-evolving threats.

The biggest internal threats

Interestingly, IT Decision Makers have some very clear views on the current threat landscape.

Biggest security threats to a business



65%	Human element e.g. making mistakes
48%	Inability to analyse security attacks to determine cogent patterns
43%	Insider threat
42%	Physical access to the company or data centre
30%	The board not taking security seriously enough
29%	Inadequate perimeter defence
23%	Lack of coherent security policy

By far the biggest internal threat, according to most ITDMs, is 'the human element' - not through malicious attacks, but through errors made by employees. This view will come as no surprise to any IT manager that has had to deal with the fallout from a lost laptop or company phone.

In an increasingly connected world, clicking the wrong website link or exposing company data on an unsecured area of the cloud, is all too easy. And while leaving sensitive printouts on a train was always a risk, today an entire company's data might be stored (and misplaced) on a single micro SD card. In other words, the 'human error' vector carries with it more risk today than ever before.

This concern with 'the human factor' underlines the need for comprehensive security policies. This is something that, thankfully, the majority of ITDMs already have in place. Periodic reinforcement of such policies (through training and other means) can go a long way to help offset the risk of human error. However, as any experienced ITDM will know, it is impossible to ever fully mitigate against the risk of careless behaviour, so it is important to twin such policies with adequate technical safeguards.

Can you even see the threats to your infrastructure?

Also interesting is the weight given by ITDMs to the inability to analyse security attacks to determine cogent patterns (where an attack has come from, how it was carried out, and via what point in the system). Data points such as these can be invaluable in understanding attacks, recognising what has been compromised, and mitigating against these attacks in the future.

Anecdotally, this inability to gain insight into security attacks appears to be a common complaint. It reveals that many companies lack both the ability to view their infrastructure in a joined-up way, and to analyse and action that visibility. This, again, reflects the growing complexity of maintaining visibility of (often cloud-based) networks and the data that runs over them, and having access to the skills required to do so.

Some of the prominent issues at the forefront in today's threat environment

BYOD

Requiring password enforcement, encryption, device management, access control, and more. Android devices are worthy of special mention due to the sheer volume of well-documented vulnerabilities that have been uncovered in recent years.

Increasingly sophisticated malware/ransomware

As long as businesses continue to pay to recover their data, agile cybercriminals will continue to run zero-day exploits and malware hiding them in common services. This includes ghostware, which attempts to hide its tracks, and Blastware.

TOR

The rise of 'the dark web', offering readily-available cover for cybercriminals.

The rise of the IoT and M2M communications

The IoT will expand to over 6.4bn devices in 2016 (Gartner) and a number of serious device security flaws have been uncovered, making this likely to remain a worrisome attack vector for the foreseeable future.

The increasing prevalence of exploitation toolkits

Hackers no longer need to be the elite group of IT experts they once were, with over 70 toolkits already 'in the wild'.

Security - the IT priority for 2016

Consequences of data breaches

Given the speed at which today's threat landscape is evolving and the growing complexity of business networks, it will come as no surprise to learn that security is top-of-mind for most ITDMs.

When asked about their concerns, 'security' was ranked first, followed closely by 'cost'. Security was also a clear priority in terms of ITDMs' spending priorities. If any budget is freed up, security is the first area in which they would spend it. This was the same in 2015 and 2014, in previous research Node4 carried out with ITDMs.

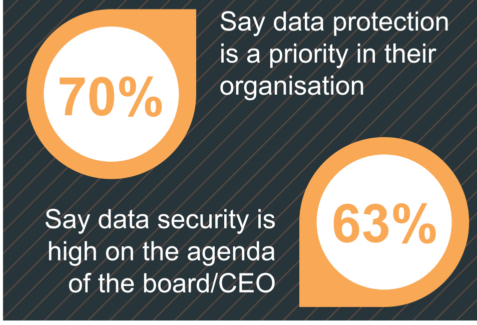
Data is the lifeblood of businesses and remains the biggest single asset to most companies. In the final reckoning, security is simply a means to an end – preventing unwanted access to, and manipulation of, sensitive company data.

Any data compromise could result in reduced profits, loss of face, or even the closure of the business.

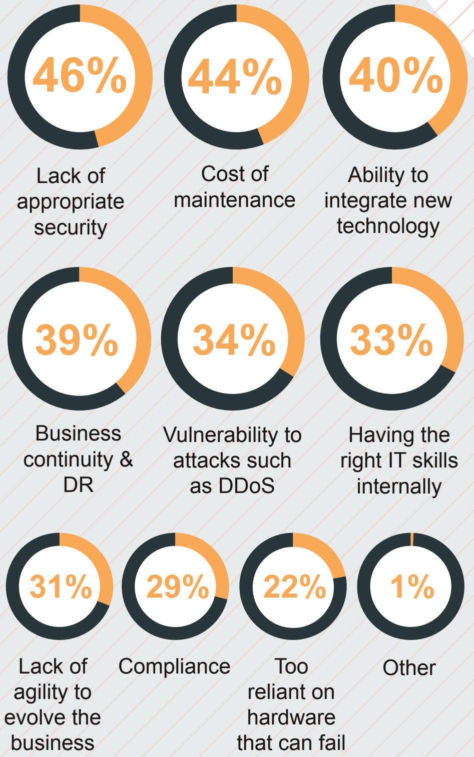
With new and ever-more stringent data protection legislation coming in around the world, the costs of getting this wrong could, theoretically, extend to fines and even incarceration. As a result, the vast majority of businesses claim that data protection is a priority in their organisation, and on the agenda of their board.

However, arguably, the measures employed by most businesses do not align well with the nature of today's security threats.

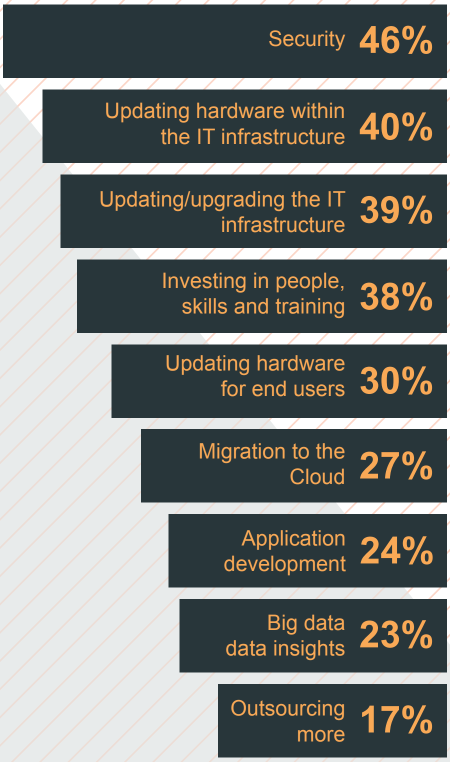
Attitudes to data protection and legislation



Concerns about IT infrastructure



Where companies would spend extra budget if it became available



NODE4
enabling business to do business

Current security strategies

How are today's IT departments approaching IT security?

So, security is the top priority for ITDMs. But what measures do they actually have in place to protect their organisations and are these enough to offer the protection today's businesses require?

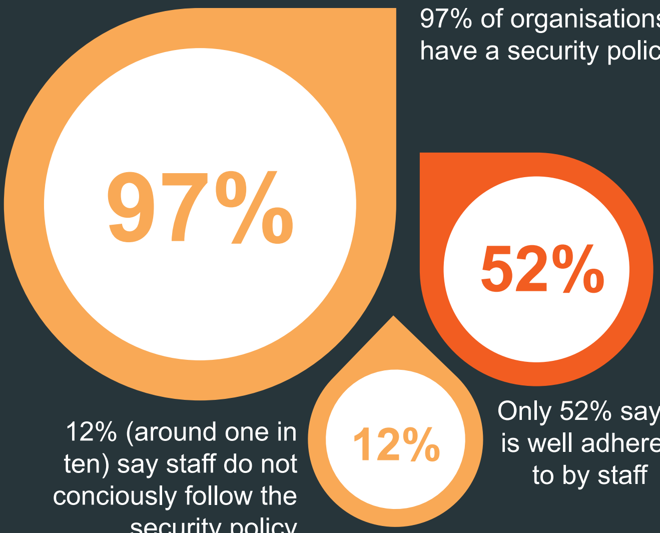
Policies and practices

At first glance, our research reveals that 63% of ITDMs conduct security assessments on their IT infrastructure. A significant 97% also say they have a security policy in place, guiding staff as to best practice.

It all sounds positive. But upon digging a little deeper, it turns out that only 52% of those organisations with a security policy say it is well adhered to by staff.

This most likely explains why ITDMs rank everyday staff members fairly low in terms of their degree of security 'savvy-ness'. On the other hand, are ITDMs doing enough to reinforce and reaffirm the security policies that they have put in place? After all, everyone has a job to do and cannot be expected to constantly consider security issues.

Security Policies



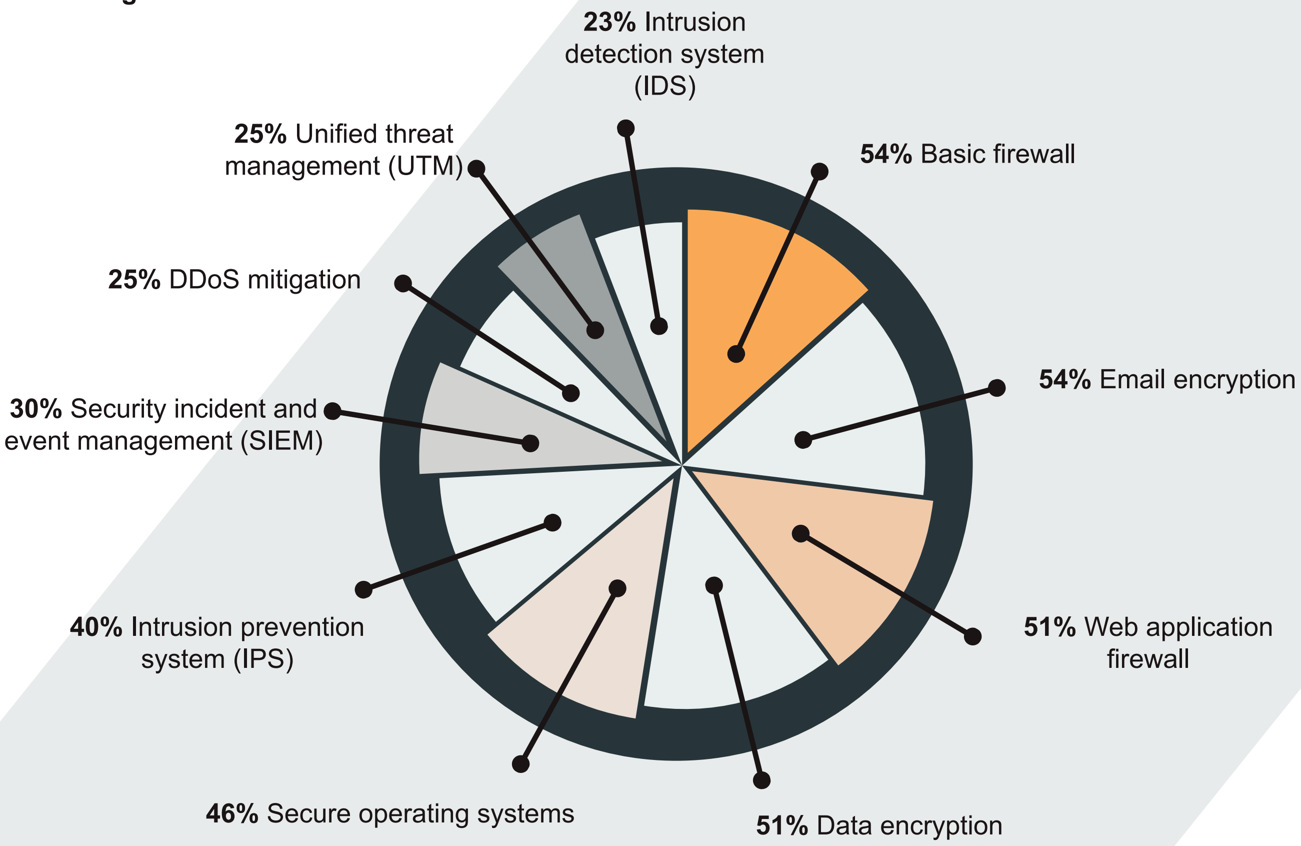
97% of organisations have a security policy

Only 52% say it is well adhered to by staff

12% (around one in ten) say staff do not conciously follow the security policy

It's entirely possible that both staff and ITDMs assume that security is a specialist remit; one in which security issues should realistically be mitigated primarily through the use of technology and the background machinations of the IT function, rather than through the user's strict adherence to policy.

The security measures in place across UK organisations



Technology

It appears that most organisations have the fundamental technological security measures in place that you might expect. The most commonly employed elements are firewalls, encryption and secure operating systems - the basic cornerstones, you might argue, of any IT security set-up.

Yet, it's interesting to note, in light of the increasing emergence of more sophisticated threats, that far fewer businesses have in place the kind of tools that would allow them to mitigate intrusion or DDoS, or to take a holistic view of their infrastructure and manage threats from within a UTM system.

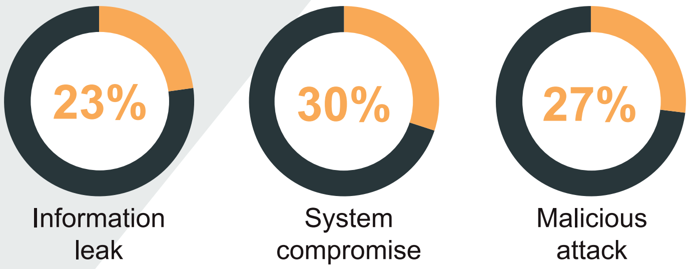
As many as three quarters (75%) of businesses have no DDoS protection in place, nor any ability to take a 'topline' view of their infrastructure.

At the simplest level, these findings suggest that most businesses are not adequately equipped to handle today's increasingly complex threat landscape. They lack the higher-end tools required to spot and mitigate emerging threats in a timely fashion. And we shouldn't ignore that nearly half of ITDMs surveyed were lacking even the most basic firewalling security measures.

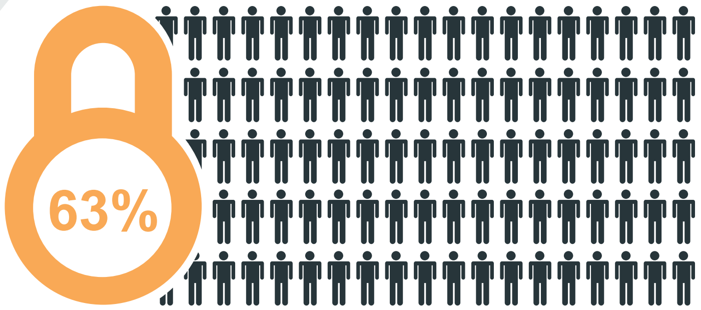
This likely explains why only around a quarter of ITDMs rate themselves as 'very confident' that they could handle issues such as 'malicious attacks', 'information leakage' or overall 'system compromise'.

Despite all this, 63% of ITDMs believe they have adequate protection at the server level to repel attacks.

Percentage of IT Decision Makers that are very confident they can handle the following:

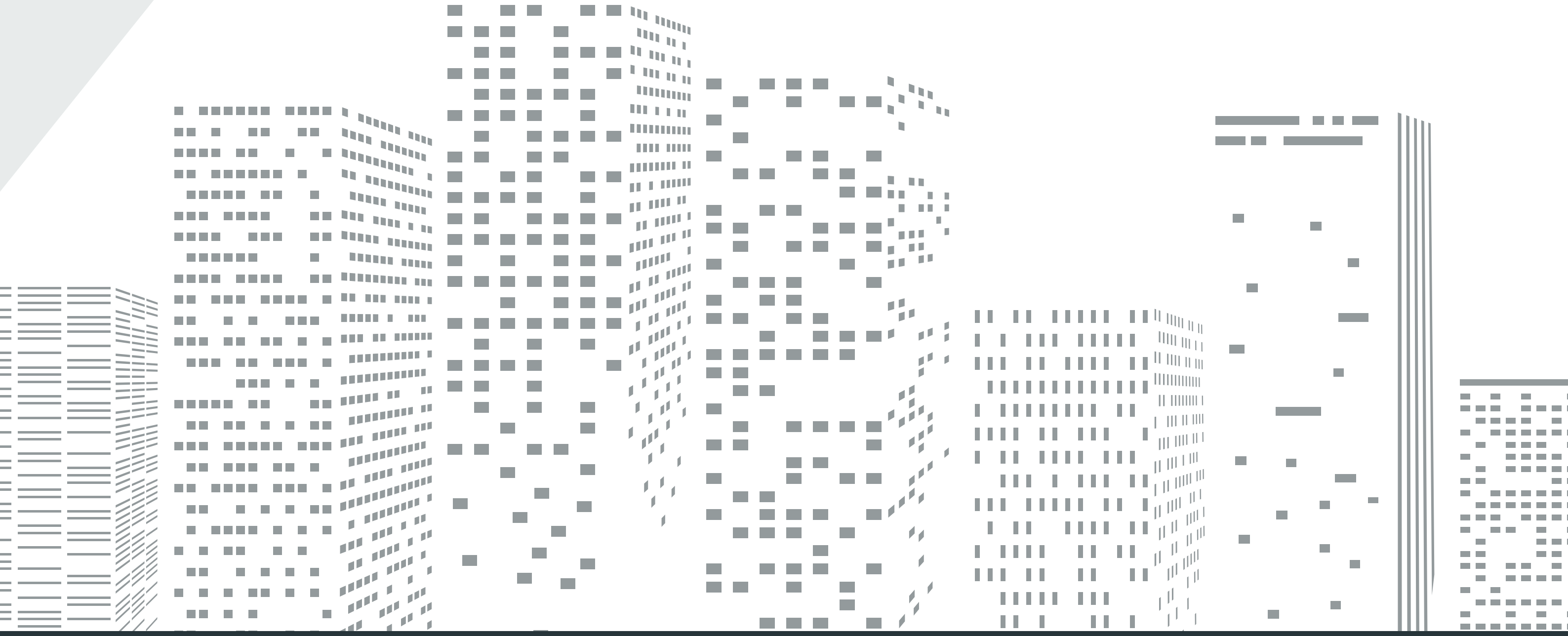


Percentage of ITDMs who believe they have adequate server level protection



This seems like an unjustified level of confidence given the facts above, and the aggressive new threats emerging.

Such disconnects may, arguably, be due to a lack of awareness of new and evolving threat vectors, and, for that matter, a lack of awareness of any incursions that may have already occurred within their infrastructures.



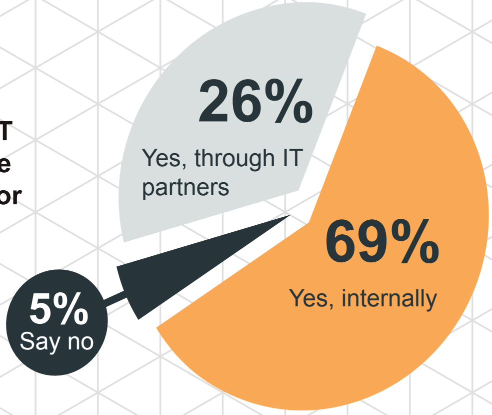
Taking control of securing the organisation

Whose role is it anyway?

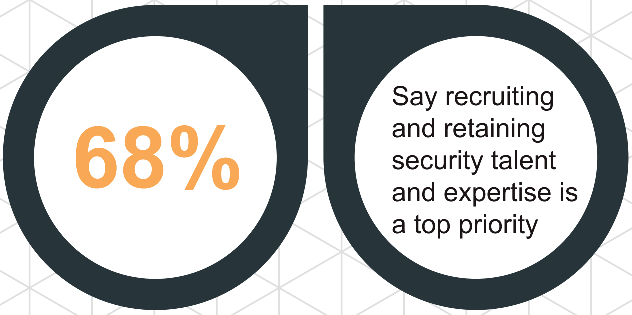
It is no surprise that ITDMs consider the IT department to be the most cyber-savvy within the organisation, closely followed by the third party or contract staff that they work with. As the typical gatekeepers of company networks and the data that runs across them, it's perhaps more reassuring than surprising.

However, confidence in the board and employees is considerably less. Given the concerns ITDMs have expressed around the 'human element', this raises potential issues. The board in particular has access to some of the most sensitive data in the company, so should they be better armed with the knowledge and skills to know how to protect and secure the information they are handling? And whose failing does this represent?

Do IT Decision Makers believe the IT function/IT department have the right skills for today's security environment?

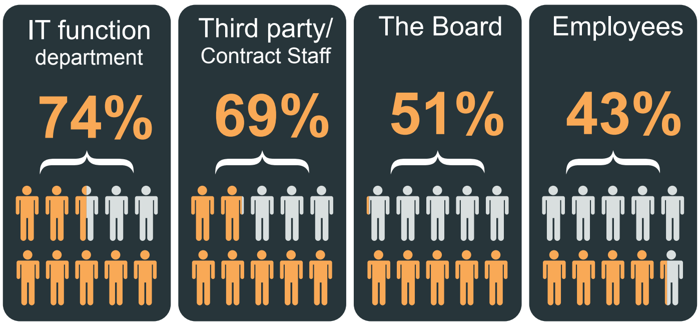


95% of IT Decision Makers believe that the IT function (both internal and partners) have the right skills to deal with today's security landscape. That said, ITDMs also highlight that recruiting and retaining security talent and expertise is a top priority area. Organisations obviously recognise the importance of shoring up IT skills and knowledge as threats and cyberattacks become increasingly complex and sophisticated.



These findings align with the view that the overriding responsibility to ensure the security of a company's IT infrastructure falls on the shoulders of the IT department.

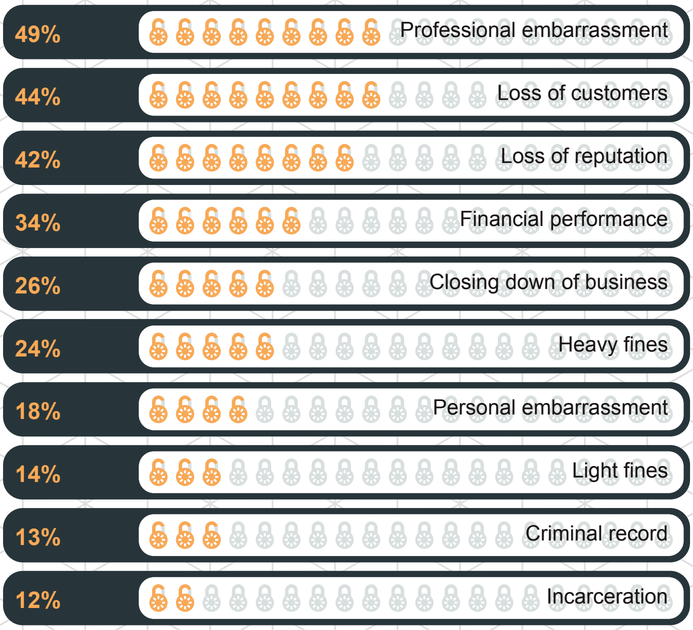
ITDMs who agree the following roles are cyber-savvy



What could be the cost of a breach?

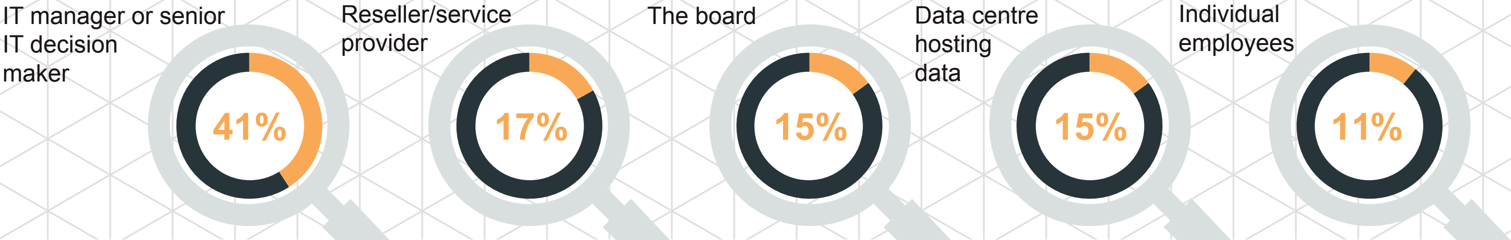
We asked IT Decision Makers to highlight what they considered to be the major consequences of a data breach. While there are clear implications on business performance and revenue, for example with the loss of customers, fines and dips in financial performance, the number one consequence is cited as 'professional embarrassment'.

The most important consequences of a data breach



ITDMs are clearly taking security seriously – and personally - and they recognise the critical repercussions of not protecting their organisations, as well as who will be 'to blame' for any issues.

Who is responsible for ensuring the security of a cloud-based IT infrastructure?



IT security strategies

Understanding levels of confidence in current approaches

ITDMs may understand the repercussions of not protecting their organisation, and are ready to take responsibility for any failures - but how confident are they in their current security approaches?

The research shows that there is a huge difference in IT Decision Makers who are 'fairly confident' in handling certain security issues compared to those who are 'very confident'. For instance, 78% of IT Decision Makers are fairly confident that they can handle an information leak, whilst only 23% could confirm they are 'very confident' that they can do so.

In addition, only around quarter of IT Decision Makers rate themselves as 'very confident' that they could handle specific problems such as malicious attacks, information leakage and/or overall system compromise.

A data breach can be highly detrimental to a company, so any doubt over the effectiveness of a security strategy is obviously of concern.

Level of confidence in handling security issues

Information leak
Fairly confident
78%
Very confident
23%

System compromise
Fairly confident
87%
Very confident
30%

Malicious attack e.g. DDoS
Fairly confident
82%
Very confident
27%

Natural disaster/ unexpected event
Fairly confident
80%
Very confident
29%

Compliance & data protection
Fairly confident
93%
Very confident
47%

Scale for future needs of the organisation
Fairly confident
84%
Very confident
25%

Identifying & mitigating insider threats
Fairly confident
81%
Very confident
21%

Lack of visibility into security could result in the failure of the business

Given the less than inspiring levels of confidence in current security approaches, it's no surprise that 41% of ITDMs do not know how many intrusions or security breaches their organisation has suffered in the last twelve months.

The consequences of inadequate threat management and a lack of visibility into the network could have far reaching consequences. A significant 83% of ITDMs cite that their organisation couldn't survive longer than 24 hours without its critical infrastructure.

41%
of ITDMs lack visibility of attacks

83%
of organisations wouldn't survive 24hrs

How long an organisation could survive without its critical cloud-based infrastructure

6%	5%	15%	24%	23%	9%	12%	6%
Less than 30 mins	30 mins - 1 hr	1 - 2 hrs	2 hrs - 12 hrs	12 hrs - 24 hrs	24 hrs - 48 hrs	More than 48 hrs	Indefinitely

Creating an IT security strategy

Best practice approach to protecting your organisation

It's clear that, despite their concerns, most organisations aren't doing as much as they could to mitigate security risks in today's data-led world.

Even for the most seasoned of security professionals, it's crucial to keep in mind the basic elements of security best practice. But in today's complex threat landscape, going beyond the basics is increasingly important for any IT security strategy.

1

Audit continuously and establish policies accordingly

The first step any organisation should take when developing a security strategy is to assume from the outset that they will be a target and develop policies accordingly.

Organisations should also perform a comprehensive audit that assesses the needs and vulnerabilities of existing infrastructures, allowing them to anticipate and mitigate potential threats before they happen.

2

Establish visibility over complex infrastructures with SIEMS

In mitigating threats, organisations need to be able to deal with the growing complexity of modern infrastructures. Today's businesses increasingly combine their own private networks with elements of cloud and colocation. It is increasingly important to implement a Security Information and Event Management (SIEM) strategy that takes a birds-eye view of pertinent data from a single point, regardless of location. Surprisingly this is an approach that a minority of (even large) organisations is currently carrying out.

3

Make sure you cover the basic technological solutions (and shore up your perimeter defenses)

Next Generation Firewalls remain the beating heart of any security architecture. And as the need to perform 'deep inspection' of application-specific traffic in real time increases, so such systems are increasing in sophistication. We're likely to see increased use of ASIC-based firewalls that can offload processor tasks in order to minimise processing bottlenecks.

Yet despite the core importance of firewalling only around half of organisations surveyed claim to have some form of firewall in place. In fact, today's perimeter defence should go well beyond firewalling.

Businesses should seriously consider the use of Unified Threat Management, which can allow them to effectively mitigate a wide range of threats and intrusion methodologies and collate the various security threats and control policies behind

5 key points to remember

1. Audit continuously and establish policies accordingly
2. Establish visibility over complex infrastructures with SIEM
3. Cover the basic technological solutions (shore up your perimeter defenses)
4. Consider bringing in additional skills (perhaps via a managed security specialist)
5. Think about security holistically

a single pane of glass. Additional systems to consider include Intrusion Prevention Systems and Data Leak Prevention. Again, worryingly, fewer than a quarter of all businesses surveyed currently have such systems in place.

The fact is that any security precautions need to be fairly comprehensive in order to adequately match the scale and sophistication of the threats posed. Any comprehensive security strategy will necessarily draw in many other additional components. These might include DDoS protection, a secure operating system choice, anti-virus software, anti-malware, spam protection, email filtering, phishing protection, secure encrypted remote access, secure authentication, application control, sandboxing, load balancing, QoS, and too many others to mention.

Any security technology needs to be wielded with experience in the context of stringent corporate policy and a sound network design. A locked front door is of no use if the side window is left open.

4

Consider bringing in additional manpower/ skills (via a managed security specialist)

Overall, managing IT security is becoming an increasingly complex task, and one that can require significant investment of manpower and skills.

Given that dedicated security strategists are a luxury that cannot afford, it may make sense for many organisations to consider managed security services, tapping into the skills and expertise that they can't access internally.

5

Think about security holistically

Finally, it's important to take a holistic approach, ensuring features are part of an overall security structure that encompasses employee awareness, policy enforcement, and ongoing penetration testing and risk analysis.

Conclusion

Assess and evolve security policies

IT professionals attempting to address security today face considerable pressures. The number of potential attack vectors is increasing day-by-day. Businesses are becoming ever more connected, with an increasingly heterogeneous mixture of on-site architectures, cloud systems, and growing exposure to a rich mix of employee devices. And at the same time, malicious parties are growing increasingly aware of both the potential worth of businesses data and of potential vulnerabilities. The costs to any business of getting security wrong could be considerable.

It’s clear that ITDMs recognise this and are working hard to keep up.

We would argue, however, that, while ITDMs may feel confident that they’re meeting the challenges of today’s security environment, most are taking too few precautions. Addressing security threats today demands a greater wealth of skills and resource than ever before, and too often ITDMs are relying on fairly ‘traditional’ security solutions. Newer threats need to be met with newer approaches. In the near future, we believe this is likely to involve a sharp growth in the use of ‘single view’ security systems, SIEM, and security managed services.

In an ever-changing security landscape, IT Decision Makers need to consider whether their systems and strategies adequately future proof them against current and emerging threats. Organisations must continuously assess and evolve their security approach in light of best practice recommendations in order to address both present and future security challenges.

CLOUD

COLOCATE

CONNECT

COMMUNICATE

MANAGED SERVICES

About Node4

Node4 is a UK-based Cloud, Data Centre and Communications specialist that is dedicated to serving its customers to ensure that they benefit from the most effective and flexible application of technology. Since 2004 Node4 has achieved great success and growth based on its focused customer service, market leading customer retention and comprehensive service offering, achieving an annual turnover of nearly £30 million.

In addition to offices in Reading, Newark and London, Node4 owns and manages Data Centres located in Derby, Leeds and Northampton, which has a PUE of 1.1, as well as having dedicated space in a Slough Data Centre. The Data Centres are connected using Node4's national fibre network, recently upgraded with a multi-million pound installation of DWDM, which includes points of presence in Manchester and London, as well as interconnects to major UK carriers. Using this infrastructure, Node4's offerings include Cloud, Colocation, Connectivity, SIP, Hosted Unified Communications and Managed Services.

For more information, visit: www.node4.co.uk.

LLOYD'S REGISTER QUALITY ASSURANCE ISO27001

HM Government
G-Cloud
Supplier

NODE4

☎ ✉ 🌐

0845 123 2222 | info@node4.co.uk | node4.co.uk

enabling business to do business