NTT Security

# Business Security:
# Always a Journey, Never a Destination

## 2017 Risk:Value Report

# Executive Summary

Businesses face an unprecedented set of information security risks in 2017. Not only are companies suffering a growing number of data breaches, but also the compliance risks are mounting. Organizations must address cybersecurity and privacy, not just because they face financial and reputational fallout if they don't, but also because regulators can penalize them for inadequate protection.

Against this backdrop, NTT Security interviewed 1,350 decision makers in businesses across the globe to find out how they viewed information security risk, and what they were doing to mitigate it. We asked questions ranging from their awareness of compliance issues to how securely they stored their data.

This year's NTT Security report featured questions in several key areas, including where data was physically stored, the impact of new compliance requirements, and how well businesses communicated information security policies to staff. It broadens an already comprehensive picture of global cybersecurity preparedness.

The results from the research are mixed. On the one hand, companies are making headway in the fight to secure their data. They are showing improvements in key areas, such as storing data securely, investing in cybersecurity measures and cyber insurance.

On the other hand, there are several gaping holes in other aspects of cybersecurity preparedness. Companies are unaware of how or even whether security-related regulations affect them, and are still behind in the creation and communication of information security policies.

As the stakes rise for businesses in Europe and beyond, with the impending General Data Protection Regulation (GDPR) they must bite the bullet and invest in cybersecurity. This isn't simply a financial exercise. It also takes an inspired and engaged workforce to create a cultural shift within the organization. Cybersecurity is a journey, not a destination.

# Introduction

This year's NTT Security ***Risk:Value*** report comes at a critical point for businesses. The GDPR will come into force on 25 May 2018, leaving companies with less than a year to comply with strict new regulations around data privacy and security[1].

Against this backdrop, NTT Security gauged the cybersecurity concerns and practices of companies around the globe, to better understand how they viewed regulatory compliance, and how their current practices supported it.

Many global companies are still unaware of how they will be affected by GDPR, and certainly don't understand the implications of the new rules. They are wide ranging, altering everything from the gathering of consent to where data is transferred, and how much access individuals have to it.

**GDPR's requirements are far too numerous to list in their entirety, but include[2]:**

- Individuals' rights to gain access to data stored about them, to transfer it to a third party, and to have it deleted
- Individuals' rights to complain about how their data is being processed, and to restrict its use
- A requirement to report data breaches and a description of the measures taken to regulatory authorities within member states, and in some cases to the individuals affected
- Appointing a Data Protection Officer responsible for overseeing privacy within the organization
- Adopting 'privacy by design' to show that businesses have adopted data protection techniques within their information processing systems.

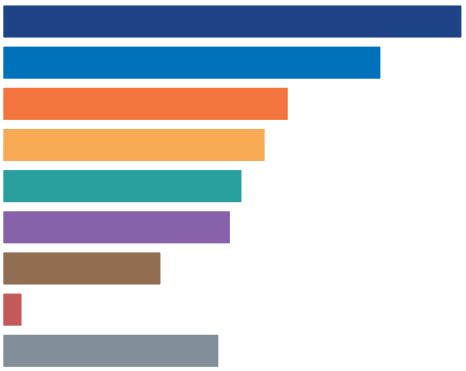
The regulations also continue existing restrictions on what data is transferred internationally, to where, and how. The difference now is that violation of some rules could result in penalties of up to €20 million or four percent of global annual turnover, whichever is the greater. This poses a very real threat to businesses that deal with the personal data of EU citizens.

With this in mind, it is more important than ever that businesses adopt appropriate information security processes and technologies to protect themselves and their customers from compromise. How do they view the current risks surrounding information security? What have they done to mitigate those risks?

*1. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
*2. https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en*

## Flying Blind on Compliance Requirements

**Figure 1** 'Which compliance regulations are your organization subject to?', *asked to all respondents (1,350), HITECH/HIPAA (Health Insurance Portability and Accountability Act) was only seen by those in the healthcare sector*



**40%** EU GDPR (General Data Protection Regulations)
**33%** ISO27001/2 (Information Security Management standard)
**25%** DPA (UK Data Protection Act)
**23%** PCI-DSS (Payment Card Industry Data Security Standard)
**21%** SOX (Sarbanes Oxley)
**20%** FCA/FSMA (Financial Conduct Authority)
**14%** GLBA (Gramm-Leach-Bliley Act)
**2%** HITECH/HIPAA (Health Insurance Portability and Accountability Act)
**19%** I don't know

### The research conducted by NTT Security suggests that many companies are still unaware of how much emerging security-related regulations will affect them. A common misconception of GDPR is that it only affects EU companies. This is inaccurate. It affects any company that processes data about EU citizens, and promises to have a profound effect on organizations across the globe.

Even in Europe, barely half the companies seemed aware that they were subject to the Regulation. Respondents in Switzerland were the most aware (58 percent) with those in Germany and Austria coming a close second (53 percent).

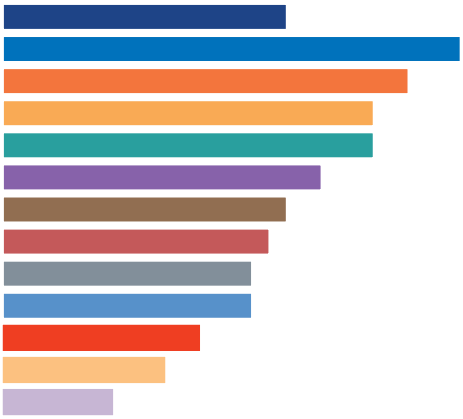
Worryingly, the lowest level of awareness in Europe seemed to be in the UK, where only 39 percent of companies identified GDPR as a compliance issue.

UK businesses will be subject to the regulation before the Brexit measures take them out of the European Union, and even then they must be compliant when dealing with countries in the EU. One in five UK decision maker respondents confessed that they didn't know which compliance regulations their organization was subject to at all.

Countries outside Europe were even less informed about GDPR. The lowest level of awareness was in the US, where just a quarter of respondents felt that it affected them. Similarly, in Hong Kong (29 percent), Australia (26 percent) and Singapore (33 percent), awareness of GDPR compliance is low. They are in for a rude awakening in May 2018 when penalties for non-compliance could run to billions of dollars for the largest organizations.

## Small Gains in Secure Data Storage

**Figure 2** Analysis of respondents that do not know where their organization's information/data is physically stored, all respondents (1,350), split by sector



**33%** Total
**53%** Government
**47%** Consumer services
**43%** Retail, distribution and transport
**43%** Utilities (including oil and gas)
**37%** Healthcare (public and private)
**33%** Business or professional services
**31%** Telecoms
**29%** Biotechnology, chemicals, petrochemicals and pharmaceuticals
**29%** Financial services, banking and insurance
**23%** Manufacturing
**19%** Computer services and technology
**13%** Construction and mining

### Data management and storage is a particularly important issue under GDPR. One key piece of advice from the UK Information Commissioner's Office (ICO) is for organizations to map their data assets so that they know what they are dealing with[3].

Companies must still try harder. In 2017, 47 percent of companies claim that all of their critical data is securely stored, which is a relatively small increase over 2015's 40 percent. More than half of all companies still cannot make this claim, which may present them with compliance challenges.

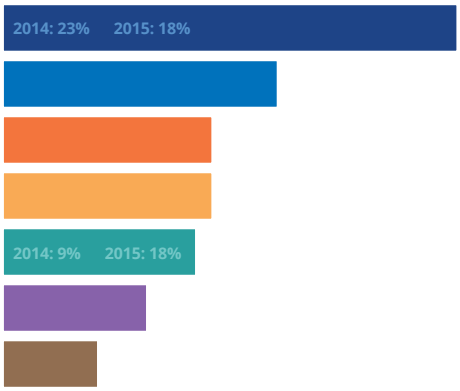
Why are these numbers still so low? You can't protect what you can't see. Just two thirds (67 percent) of respondents know where their data is held, meaning that a third of the response base faces a lack of visibility when it comes to data protection. UK decision makers are comparatively more blinkered: 43 percent don't know where their data is physically located.

Knowing where data resides is a start, but there is more work to be done. Of those that know where their data is, fewer than half (45 percent) definitely believes that new regulations will affect their data storage.

*3. https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf*

## Investing in Security

**Figure 3** 'What do you see as the single greatest risk to your business?', *asked to all respondents (1,350)*



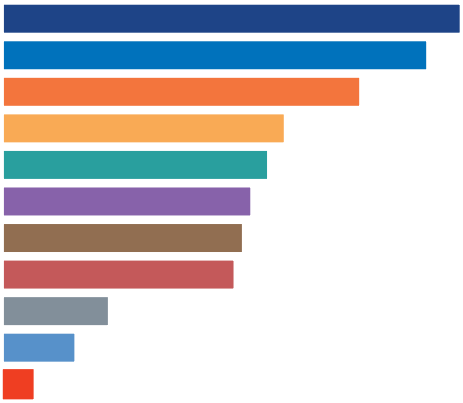

**28%** Competitors taking market share
**17%** Lack of employee skills in key areas
**13%** An increase in global competition
**13%** Decreasing profits
**12%** Poor information security
**9%** Budget cuts
**6%** Industry disruption caused by new technologies, e.g. internet of things

This lack of visibility isn't creating as much concern as onlookers might expect. Companies aren't acknowledging information security enough in their risk assessments. In 2015, almost one in five decision maker respondents (18 percent) considered poor information security to be the single biggest risk to their business. In 2017, that number fell to one in eight (12 percent) and took fifth place, behind losing market share to increasing global competition, eroding profits and unskilled employees.

One reason why companies might be less worried about information security risk is that they feel protected by increased investment. In 2015, they allocated 12.66 percent of the IT budget and 10.59 percent of the operations budget to information security. That rose substantially to 14.58 percent and 15.53 percent respectively in 2017. Companies are spending more on cybersecurity, but are they safer?

## Assessing the Risk

**Figure 4** 'If information was stolen in a security breach, how would your organization be affected?', *asked to all respondents (1,350)*



**55%** Loss of customer confidence
**51%** Damage to brand/reputation
**43%** Direct financial loss
**34%** Loss of shareholder value/share price
**32%** Financial penalty from an industry body or government
**30%** Loss of investment/potential investment
**29%** Disciplinary action against employees
**28%** Reduced business growth
**13%** Staff loses (to join other companies/competitors)
**9%** I/other senior decision makers in the business may resign
**4%** We wouldn't suffer any impact

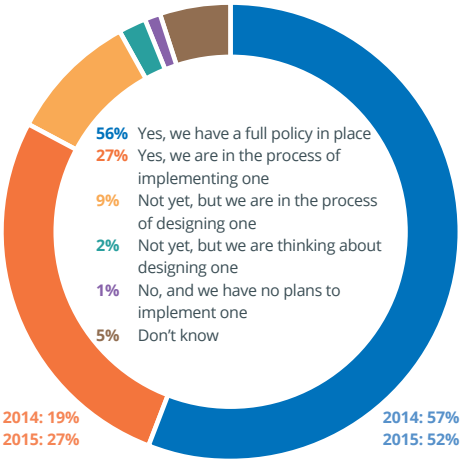
Respondents to the NTT Security research didn't seem to feel safer. 57 percent of them believe a data breach is inevitable at some point. If and when it happens, the impact will be two-fold: companies expect news of a breach to affect their longer-term ability to do business, and also to have a more direct short-term financial impact.

43 percent of respondents believed that they would suffer direct financial losses from a breach, while 34 percent predicted an erosion of shareholder value, but the most anticipated effects were cultural. 55 percent of them said that a breach would affect customer confidence, followed by brand and reputation (51 percent). This correlates with their top perceived business risk: losing market share to others.

Companies are right to worry about the short-term impact on business revenues and the longer-term cultural impact of a breach. The estimated cost of recovery, on average, has increased from $907,000 in 2015 to $1.35m in 2017. While the estimated impact on business revenue has decreased from 2015's 12.51 percent, it is still significant today, at 9.95 percent. No company can afford to lose a tenth of its revenue.

# Information Security Policies: More Work Needed

**Figure 5** 'Does your organization have a formal information security policy?', *asked to all respondents (1,350)*




## Companies can drive a culture of security throughout their organizations by creating information security policies that guide staff in how to deal with data.

If security is to become part of a company's culture, it must begin at the top with boardroom support. Companies seem to understand this in theory, with almost three in four (73 percent) suggesting that preventing a security attack should be a regular item on the boardroom agenda.

In practice, though, things are very different. Just 56 percent of the respondents noted attack prevention as a regular topic of discussion among C-suite executives. This tells us that overall, cybersecurity needs more executive airtime.

This lack of visibility at the board level is trickling down into the rest of the organization. Many companies lack direction when it comes to information security. Just over half (56 percent) of respondents identified a formal information security policy at their company. This is slightly up from 52 percent in 2015, but still far short of where it should be.

Formalizing information security always seems to be a work in progress. 27 percent of companies are partway through implementing an official information security policy. This hasn't changed since 2015. The clear message: "We're working on it." But how much of a priority is it?

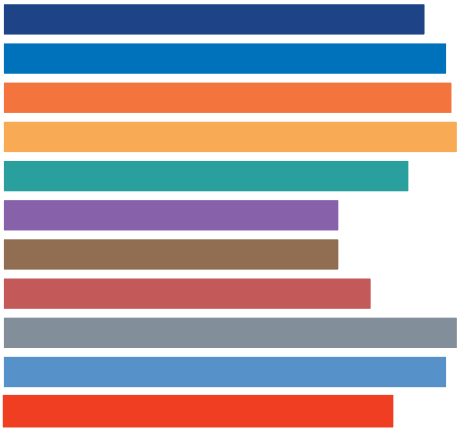
The percentage of respondents with an official information policy was unevenly distributed on a per-country basis. While some companies dragged their heels (in particular Sweden, with just 30 percent) others excelled. The UK led the field by far, with 72 percent of companies claiming an official policy.

On a per-sector basis, healthcare led the way, with 69 percent of companies claiming an official information security policy. Finance came a close second (66 percent).

One worrying statistic was in consumer services, where barely more than a third (35 percent) had an official policy. As a sector dealing with sensitive personal data, this leaves companies and their customers open to attack.

# Communication and Awareness

**Figure 6** 'Has the information security policy been actively communicated to everyone in the organization?', *respondents who answered 'yes' by country (594)*



**79%** Total
**83%** UK
**84%** US
**85%** Germany and Austria
**76%** France
**63%** Sweden
**63%** Norway
**69%** Switzerland
**85%** Hong Kong
**83%** Australia
**73%** Singapore

## Security policies aren't useful if they're kept locked in a drawer. They should be living, breathing documents, regularly updated and reviewed. More importantly, they should be understood by staff who are dealing with potential security situations on a daily basis. The UK Government highlights employee awareness training as one of ten cybersecurity steps in its best practice guidelines.[4] How well is the global business community communicating these principles?

Of those with a formal policy, eight in ten (79 percent) said that they had actively communicated the information security policy to everyone in the organization. Germany and Austria did particularly well, with 85 percent of respondents rising to the challenge. The US (84 percent) and the UK (83 percent) also outperformed the average.

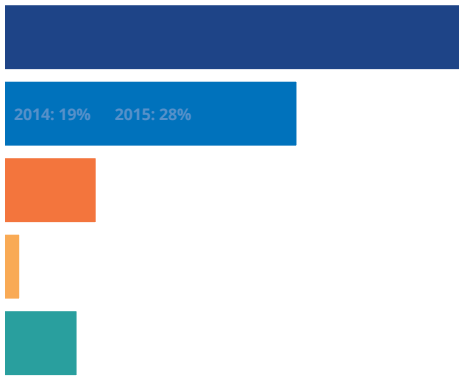
These figures don't acknowledge the quality of communication, though. Dropping a PDF file in someone's in-box doesn't constitute an awareness program. Companies may be communicating information security policies, but in practice, NTT Security's research showed that just 39 percent of employees are fully aware of their organization's information policy.

However, these communication and awareness figures only reflect responses from the 56 percent of organizations that have an information security policy in place. This means in reality that only 44 percent of companies have communicated an information security policy to their employees, and barely one in five companies (22 percent) believe that their employees fully understand them. The business community has some work to do.

*4. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary*

# Incident Response

**Figure 7** 'Do you have an incident response plan in the event of a security breach or of non-compliance of information/data security regulations?', *asked to all respondents (1,350)*




**48%** Yes, we have an incident response plan
**31%** Yes, we are in the process of implementing an incident response plan
**10%** Not yet, but we are in the process of designing an incident response plan
**2%** No, and we have no plans to implement one
**8%** Don't know

One of the biggest issues for a company hit by a security breach is the time it takes to recover. This has a direct effect on the resilience of the business, which is a crucial factor. Businesses unable to weather the storm of a cybersecurity breach lack resilience and can even cease operations as a result. There have been several examples of hacks killing companies.[5] Respondents expect to take over two months (74 days) to recover from a breach, on average.

The speed of recovery relates to how well a company plans for an incident. An incident response plan is a crucial part of any company's cybersecurity preparedness program. Unfortunately, less than half of the companies surveyed (48 percent) have one, although another 31 percent said that they were implementing one.

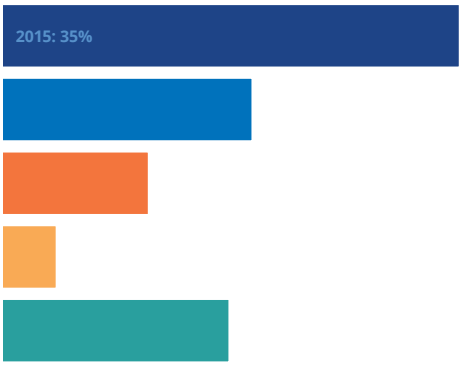
How effective are these response plans likely to be? It depends on whether anyone reads them or not. Of the companies that had or were implementing a full plan, just 47 percent of respondents fully understood what was in it. Another 47 percent were "partly aware".

One promising thing here is that the C-suite plays an active part in executing the response plan. They allocated responsibility fairly evenly between the CEO (23 percent), CIO (21 percent), CISO (22 percent), and COO (21 percent). This means that, to some extent, breach preparedness is getting the executive attention that it needs.

*5. https://www.infosecurity-magazine.com/magazine-features/killing-me-softly-with-his-hack/*

# Interest Grows in Cyber-Risk Insurance

**Figure 8** 'Do you have a dedicated cyber security insurance policy?', *asked to all respondents (1,350)*




**40%** Yes, we have a dedicated cyber security insurance policy
**22%** No, but we are in the process of getting one
**13%** No, but we are thinking about getting one
**5%** No, and we have no plans to get one
**20%** Don't know

Cyber-risk insurance is a way to mitigate the risks of cyber-compromise. In 2015, 35 percent of companies had such a policy, while 43 percent were either getting one or considering one. Two years later, that interest hasn't translated into action. Slightly more respondents than in 2015 – 40 percent – have cyber-risk insurance, while 35 percent of companies are now getting or considering it.

The sectors that have embraced cyber-risk insurance the most are those with sensitive intellectual property or customer data. 52 percent of financial institutions have it, followed by 51 percent of those in the biotech/chemical and pharmaceutical sector. Those lagging behind include utilities (20 percent), government (25 percent) and consumer services (26 percent).

## Poor Practices Put Insurance at Risk

Cyber-risk insurance is a popular trend in business circles, but such contracts can be difficult to negotiate, with many variables. Insurance companies expect a certain level of cybersecurity maturity from the client. If companies can't demonstrate their competence in basic cybersecurity and risk management, they may fail to secure a contract or may find an existing one invalid.

Respondents to NTT Security's research acknowledged multiple risks that might endanger cyber-risk insurance contracts.

**Poor system patching.** 45 percent of companies felt that failing to patch existing IT systems would or could invalidate their company insurance. This is one of several basic cybersecurity practices identified by the Australian Signals Directorate that will stop the majority of attacks[6]. It was one of the biggest reasons for the spread of WannaCry, the ransomware that swept the globe in May 2017. This attack exploited software for which Microsoft had already issued a patch over a month prior[7].

**Aging IT systems.** 38 percent of companies identified this as an insurance validation risk. WannaCry primarily exploited unpatched Windows 7 systems, which were close to or past their end of life. Current operating system versions were unaffected.

**Lack of an incident response plan.** 37 percent of businesses believe that having no incident response plan would affect their insurance.

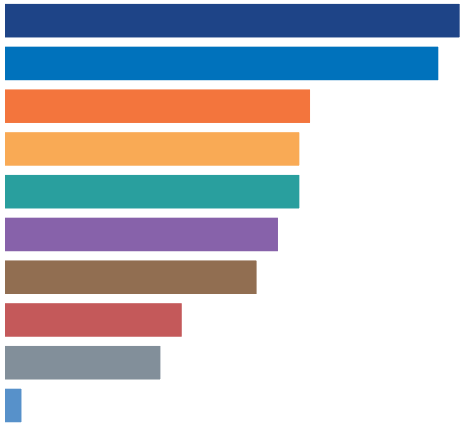
**Lack of compliance with industry regulations.** Almost a third (32 percent) of companies felt that not complying with industry regulations could or would invalidate their company insurance. GDPR could exacerbate that problem.

**Lack of employee care and attention.** 26 percent of companies felt that their employees could let them down on key cybersecurity issues, which would impact any cyber insurance policy. This highlights the need for robust, properly communicated information security policies and training.

*6. https://www.asd.gov.au/publications/protect/top_4_mitigations.htm*
*7. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx*

# Working With Third Parties

**Figure 9** 'Why does your organization currently or plan to use a third party managed security services provider?', *only asked to respondents whose organization currently, plans to or might consider using a third party (977)*



**43%** Providing data storage
**41%** Support with data management
**29%** To gain access to better technology
**28%** We have a lack of internal resources
**28%** We have a lack of internal skills
**26%** We are implementing Business Process Outsourcing (BPO) (e.g. HR & payroll, sales order processing, finance etc.)
**24%** It is cheaper to outsource
**17%** To assist with cloud migration
**15%** To assist with system modernization
**2%** I don't know

## 6 percent of companies currently have help from a third party managed security services provider, although as the challenges mount, more are considering it. 38 percent of respondents said that they are planning to bring in external help, and another 28 percent said that they might consider it in the future.

Financial services stood out as a leader here, with one in ten companies using managed security services, compared to low-single figures for most other sectors. Those sectors most interested in bringing in third party managed security services were business and professional services firms (51 percent) followed by computer services and technology companies (49 percent).

Two main things are driving the uptake of managed security services, and they both relate to forthcoming requirements under GDPR. 43 percent of those using or planning to use an external service provider wanted help with data storage, while 41 percent were looking for assistance with broader data management.

Many companies need help because they believe their own internal capabilities to be insufficient. 29 percent wanted access to better technology, while 28 percent highlighted a general lack of internal resources. 28 percent singled out inadequate internal skills as a problem, reflecting a key information security mantra: protection is about people and process, not just technology. And 24 percent of respondents believe it's cheaper to outsource than to manage their own security.

Conversely, half of the companies who don't use or plan to use third party services believe they have the internal skills they need.

Other factors included concerns around data sharing (40 percent), security (28 percent), and cost (21 percent).

# Conclusion

Businesses are making some advances in cybersecurity. They are investing more in securing their infrastructure, and more of them are storing data securely than in the past. They believe that they can recover more quickly from data breaches, and do so with a smaller impact on their revenues.

Nevertheless, there are some significant chasms to cross. Companies are still not raising cybersecurity as a board-level issue as much as they could, and they are failing to get employees on board by creating and communicating information security policies properly. And they understand that failure to patch and upgrade systems makes it difficult for them to get financial protection in the event of a data breach.

Perhaps the biggest risk of all is regulatory. Until now, companies that left gaps in their information security strategies could simply take the risk of compromise, and then cope with the problem if it arose. From 25 May 2018, they face a burden of proof. Should regulators come calling, businesses must show that they have taken adequate measures under the GDPR rules to protect their data. If they haven't, the penalties will be swift, and severe. Now is the time to address these issues and comply.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.

## Research demographics

Commissioned by NTT Security, the 2017 Risk:Value research was conducted by Vanson Bourne in March to May 2017. 1,350 non-IT business decision makers (35% at C-level) were surveyed in the US, UK, Germany and Austria, Switzerland, France, Sweden, Norway, Hong Kong, Australia and Singapore. Organizations had more than 500 employees and were selected across a number of core industry sectors. Approximately a third of responses came from the financial services sector.

## About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies — making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.