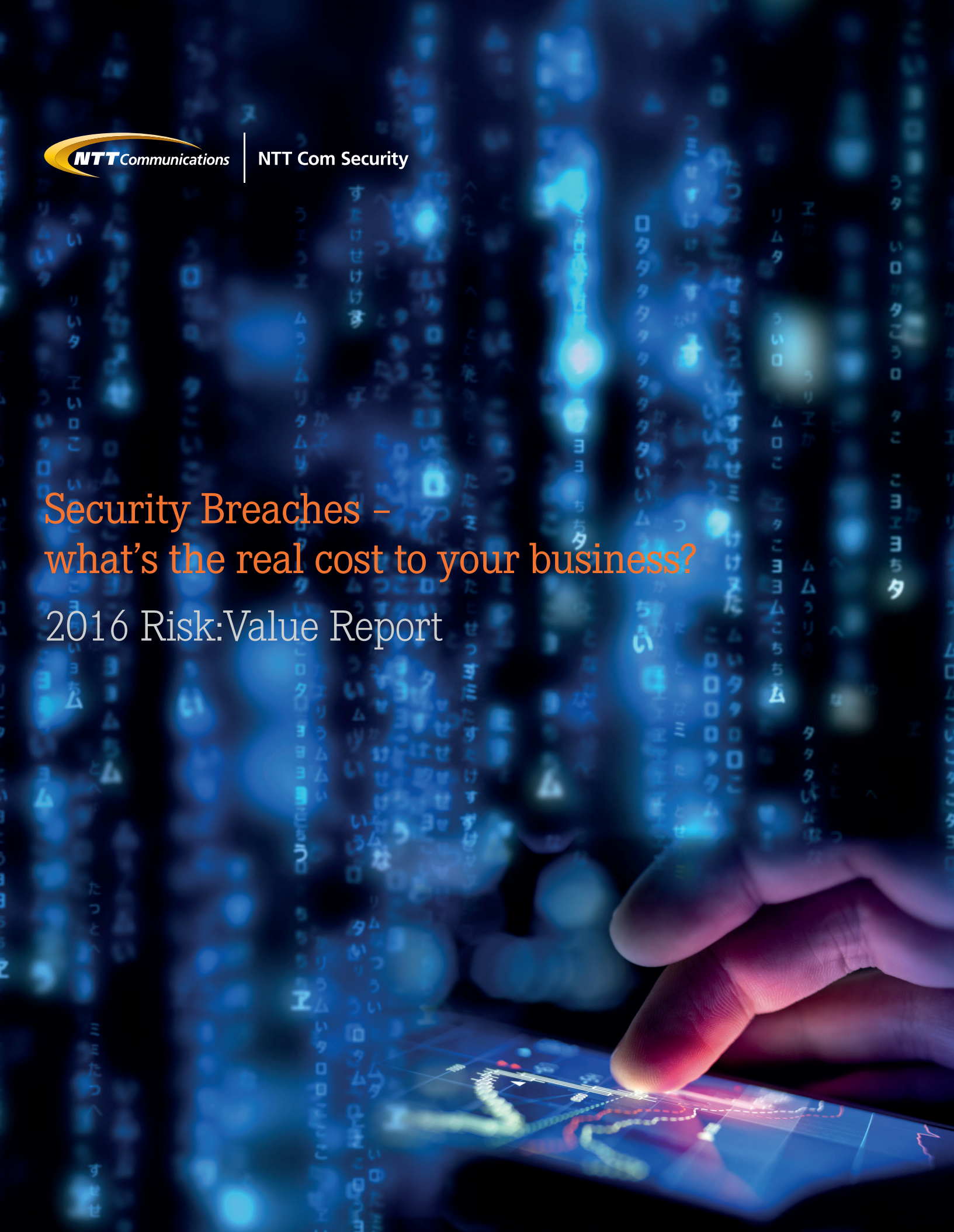
NTT Communications | NTT Com Security

Security Breaches – what's the real cost to your business?

2016 Risk:Value Report



Foreword

Companies understand the threats they face from attackers that want to steal or damage their data, but must do a better job of protecting against them if they are to avoid damaging losses. With sensitive data stored so ubiquitously in company infrastructures, the onus is on executives to ensure that it is properly shielded from unauthorized access.

In practice, companies are not putting those protective measures in place. This is leaving them open to serious implications ranging from financial losse to long-term reputational damage that will be difficult to fix.

Organizations can begin to address this problem by creating strong information security policies and communicating them effectively to employees. This will help build a secure company culture in which data breaches are prevented, rather than a reactionary one in which executives must attempt to deal with the consequences.

Executive Summary

Speeding Towards A Cliff

Study any risk-based discipline for long enough, and you will see a worrying trend: A large proportion of people understand the risk is there, but often do not address the problem until it is too late. People smoke, fail to exercise and eat bad food, while admitting that they understand the mortality statistics. On a broader scale, we know the climate change risks, but continue to burn carbon at furious rates. It's as though we are somehow programmed to procrastinate.

The same is true in cybersecurity. Organizations may understand the likelihood of an intruder stealing their data. They may even understand how badly it will impact them. But they often tend to react impulsively after the fact, rather than responding thoughtfully to a threat well in advance.

This has come through clearly in a survey commissioned by NTT Com Security and carried out by research company Vanson Bourne. It polled 1,000 business decision makers in six European countries and the US to gauge their attitudes around cybersecurity and risk. It aimed to understand the cost of cybersecurity to their business, and to find out what measures they are taking to protect themselves. Some of the results are worrying, as highlighted on the right hand side.

25%

25% of respondents are certain that their company will suffer a security breach in the future.

$1m

The security breach will cost almost $1m on average, and far more for larger companies.

75%

Three quarters of people do not believe that all of their business data is completely secure.

4 in 10

Four in ten people believe that data is more secure on their home computers than at work.

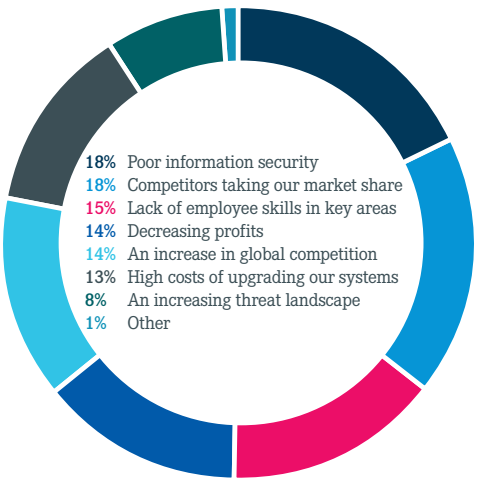
Cyber-Intrusion: A Foregone Conclusion

For many executives, it is not so much a question of whether a cybersecurity incident will occur, but when. A quarter of the participants in the survey are certain that it will happen to them, and another 40% are pretty sure that they will be hit.

Poor information security is seen as the biggest threat, with 18% of respondents highlighting it as the single greatest risk to their business, putting it on a par with competitors stealing market share. Inadequate protection of company information now beats global competition and falling profits as a business risk.

Who would have imagined this just five years ago? There is a perceptual shift in business risk, and it is happening quickly. When NTT Com Security asked businesses what their biggest risk was in 2014, just 9% highlighted poor information security. What has changed?

Figure 1 "What do you see as the single greatest risk to your business?" – *asked to all respondents (1,000 respondents)*



A Changing Security Landscape

Perceptions of business risk are accurately reflecting reality. For proof, look to the headlines. The high profile data breaches keep building, and in 2015 they ranged from the embarrassing to the financially damaging.

In February and March 2015, health insurance companies Anthem and Premera Blue Cross each announced that tens of millions of customer records had been stolen. Anthem lost 78.8 million records from its database[1], while Premera lost 11 million[2]. Security analysts suggested that the attacks may have been carried out by a single group. Then, in July 2015, hacking group the Impact Team stole 37 million customer records from adultery site Ashley Madison, holding the site to ransom and then exposing many users of the site, including several high profile individuals.[3]

So, companies understand the danger of poor security because they see the consequences in news articles each week. What are they doing to protect themselves from suffering similar breaches? The short answer is, not enough.

Understanding Without Executing

Companies understand what they must do to protect their data – at least at a high level, and in theory. The survey reveals that they could be doing it more effectively, though.

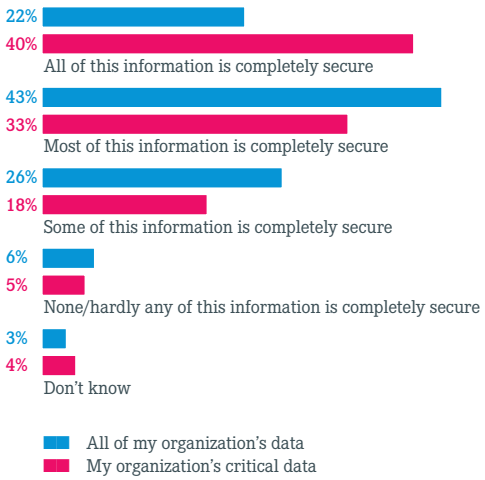
The majority of respondents associate data protection with information security, and many feel particularly strongly about it. Over half (54%) describe information security as 'vital' to their business.

Three quarters of respondents highlight this as one of the three words and phrases they are most likely to associate with information security. With 'personal privacy' – a concept closely related to personal data protection – also in the top three, it is safe to say that a data-centric information security policy should now be considered the norm in any cybersecurity practice.

For the most part, companies also understand what type of data is most sensitive. Respondents pinpoint consumer customer data and business customer data as the most important to protect, followed closely by operational data. Somewhat worryingly, though, employee data comes comes fifth, even though employee records are just as subject to privacy laws in most jurisdictions as customer records.

In spite of this, three quarters of the respondents to the NTT Com Security survey admit that not all of their information is completely secure. Critical data is slightly more secure, but still more than half (56%) of companies are unable to guarantee that all of their critical data is protected. This points to a clear understanding of the problem, but a lack of execution.

Figure 2 "How much of the information stored by your organization is secure?" – *asked to all respondents (1,000 respondents)*



1. http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364
2. http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#2715e4857a0b3406879b2143
3. http://www.techworld.com/news/security/impact-group-leaks-data-on-up-37m-ashley-madison-adulterers-3620132/

The Importance of Policy

To better understand where we are falling short, we need to understand some of the basic components of a solid security strategy. Well-defined processes are a lynchpin for adequate security. Repeatable, documented rules and procedures should underpin everything from taking data out of the workplace to change management in the IT department, as all of them help to seal the gaps that allow security errors.

Processes that help underpin security are routinely codified in standards ranging from ISO 27001[4] to the Information Security Forum's Standard of Good Practice[5], NIST's 800-12[6] and ISACA's COBIT[7], but many organizations will select elements from these and other guidelines to create their own custom policies, perhaps focusing on specific areas as befits their own business operation.

The results from the survey are initially promising, highlighting a strong interest in refining and improving security practices within the organization. Eight in 10 respondents say that they are continuously improving and updating their information security processes and features.

Digging deeper into the data reveals some cracks in the story, however. Only half of the respondents (52%) have a full information security policy in place, with just over a quarter more (27%) reporting that they are in the process of implementing one. The rest of the participants are either at the design stage, or just thinking about it.

This leaves an alarming number of companies without a solid rule set to help steer employees and senior management through a complex and dangerous challenge.

Significantly, the lack of a policy seems to be a particularly big problem for smaller companies. Only 43% of companies with 1,000 employees or fewer have a full policy in place, compared to almost 70% of companies with over 5,000 people.

The same pattern holds true for disaster recovery plans. Slightly fewer companies are prepared to recover from a catastrophic data loss, with just 49% having a full recovery plan. Again, smaller companies are far less prepared than larger ones.

4. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
5. https://www.securityforum.org/tool/the-standard-of-good-practice-for-information-security/
6. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
7. http://www.isaca.org/cobit/pages/default.aspx

Communication is Key

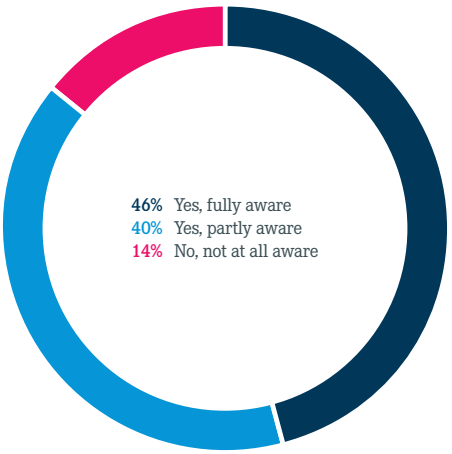
Even those organizations with a plan to recover from a security breach may not be able to follow them effectively. The best laid plans are worthless unless people know how to follow them. Yet, overall, more than half of all respondents are not fully aware of what is in their organization's disaster recovery plan, and 14% have no idea what would be needed of them in the event of a catastrophic data loss.

There is a significant reversal between small and large companies when it comes to communicating policies. Larger companies tend to have disaster recovery plans more than smaller firms, but fewer of their executives know about them.

In those companies with more than 5,000 employees that have a disaster recovery plan, just 32% of executives are fully briefed on them. Conversely, 47% of executives in companies with 1,000 employees or fewer know what is in their disaster recovery plan.

This may show the difficulty in communicating policy effectively in larger companies with more complex management structures. Regardless, the overall figures are depressing. Organizations must communicate their policies more effectively.

Figure 3 "Are you aware of what your organization's business/disaster recovery plan includes?" – *asked to those whose organization has a business/disaster recovery plan or is implementing one (772 respondents)*



Breach Recovery Can Be Expensive

If companies are not stepping up and fixing their security loopholes by building and effectively communicating policies, then what will happen when disaster strikes? The NTT Com Security survey reveals a variety of potential impacts, ranging from a direct effect on the bottom line, through to 'softer' issues, such as reputational damage.

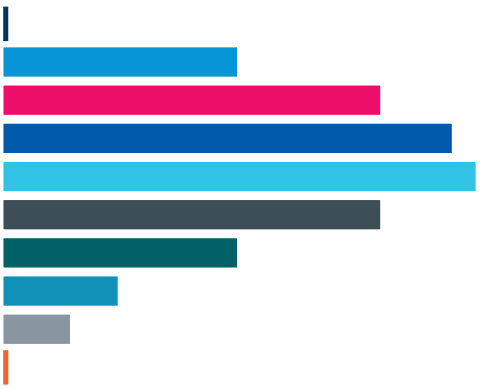
First, the financial impact. Although the majority of those surveyed could estimate the cost of recovering from a security breach, 20% did not know. On average, a breach would cost companies just short of $1m ($907,053). As you might expect, the cost varies by company size, with larger companies anticipating more financial damage than smaller ones. Companies with fewer than 1,000 employees are still liable for significant financial losses, though, averaging $362,550. Companies with more than 5,000 employees anticipate losing $1,465,976.

The disparity between different vertical sectors is also notable. Computer services and technology companies anticipate losing far more from a breach than others, averaging $2,708,438. Retail, distribution and transport companies come in second, with losses of $1,037,103. Between them, these two sectors drive up the average significantly.

This indicates that the cost of a data breach maps to a company's revenues. Other responses from the survey participants bear this out, as they directly correlate loss of records in a data breach with a loss in sales.

On average, respondents believe that revenue will drop by an eighth (13%) as a result of an information security compromise – a figure that varies by less than 2% between the smallest and largest firms. This is up substantially from an overall 8% figure in 2014, and the rise probably stems from the horror stories of financial losses running into tens of millions from high-profile breaches.

Figure 4 "If your organization suffered a security breach and lost information, how much would you estimate to be the average cost of recovering from that security breach?" – *asked to all respondents (1,000 respondents)*



0% **Less than** $10,000
10% **Between** $10,000 and $50,000
16% **Between** $50,000 and $100,000
19% **Between** $100,000 and $250,000
20% **Don't know**
16% **Between** $250,000 and $500,000
10% **Between** $500,000 and $1 million
5% **Between** $1 million and $5 million
3% **Between** $5 million and $10 million
0% **More than** $10 million

Trust is Priceless

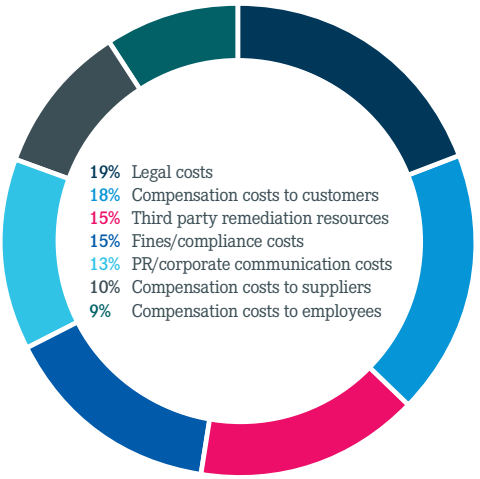
Why is the financial loss so closely correlated to revenues? Responses suggest that while direct financial losses are a significant factor, a loss of trust is even bigger.

54% of participants say that they would be affected by direct financial losses in the event of a breach, with 48% also citing financial penalties from regulators (which is in itself a financial loss). This is important, but people are even more worried about what it does to their image – and underlying sales. A full six in ten respondents point to reputational damage as a significant effect of a data breach, and 69% – the highest number of all – worry about a loss of customer confidence. If customers do not trust their supplier, they are far less likely to stay with them.

Prevention is Better Than Remediation

Survey respondents say that they would spend 13% of their remediation budget on average trying to fix an image problem via PR and communications services following a data breach. This is part of a fund heavily weighted towards dealing with the consequences of a cybersecurity breach rather than the cause.

Figure 5 *Analysis of the average percentage of how organizations' remediation costs would be split if they suffered a security breach, asked to all respondents (1,000 respondents)*



The top two costs that companies expect to spend money on after a breach are legal fees and the cost of compensating customers for the loss of their data. These take up 19% and 18% respectively. Fines and compliance costs take up another 15% of the costs incurred after a data breach, while compensation for suppliers and employees costs 19% overall.

Compared to all that, the expected cost of cleaning up and securing the company's systems and data after the fact is relatively minimal; third party remediation services make up just 15% of the anticipated breach recovery cost.

This tells us something useful: It is far more effective to prevent breaches before they happen, if possible. Addressing security issues with appropriate policies and procedures beforehand will cost less in the end than the long-running reputational and financial damage created by a breach.

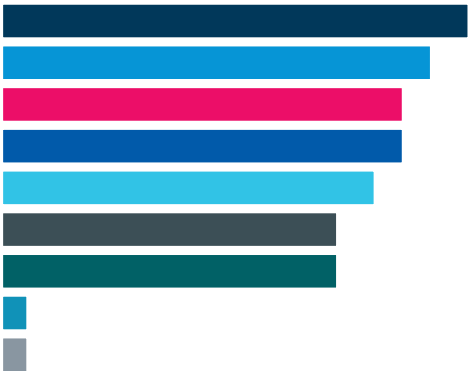
Do not underestimate just how long that damage will take to fix, either. Technical remediation, legal paperwork and compensation processes take time. On average, a company will be struggling with this for nine weeks, eating up energy that could be otherwise ploughed into growing the business. When it comes to customer confidence, the recovery could take far longer, and is difficult to measure.

Insurance: Not a Panacea

The natural thing to do when faced with risks is to look for quick-fix solutions, and one of the obvious avenues is cyber risk insurance. This is a relatively new arm of the insurance industry, with the first offerings extending back no further than the turn of this century. As such, it is still an immature space, in which underwriters and clients alike are grappling with rapidly evolving concepts.

The cyber risk insurance industry's immaturity is reflected in its uptake. Most companies are not insured against data intrusion, with slightly over a third (35%) having a dedicated cybersecurity insurance policy, although another 27% are at least actively working on getting one.

Figure 6 "For which of the following aspects, if any, do you feel would or could invalidate your company insurance?" *– asked to those whose organization has insurance cover for data loss and/or a security breach (744 respondents)*



50% Lack of compliance
46% Not complying to business policies
43% Lack of an incidence response plan
43% Lack of employee care/attention
40% Poor physical security
36% Age of IT systems
36% Lack of/poor data protection
3% None
3% Don't know

You Cannot Easily Insure Against All Losses

Even those companies that do have cyber risk insurance must consider some important caveats. One of them is the extent of their coverage. Policies often cover only particular aspects of a loss, or may simply not cover the potentially hefty amounts involved.

This comes out in the survey responses. Less than half of all participants whose companies have purchased cyber risk insurance (46%) expect it to cover legal costs, and that represents the highest proportion. Fewer (although still four in ten) expect it to cover regulatory and government fines and remediation. Covering the loss of business and intellectual property is even less likely, at just 25%.

The other issue to consider is whether their coverage is even valid. A full half of all respondents whose companies have purchased cyber risk insurance believe that a lack of compliance with the necessary security criteria could invalidate those policies. Over four in ten (43%) say that the absence of an incident response plan could invalidate their insurance and just over a third (36%) worry about the effect of poor data protection on their coverage.

Conclusion: A Well-Rounded Policy

All of this points to a simple fact: Trying to treat the symptom will not solve the cause. Companies can adopt insurance policies by all means, but it must complement rather than replace a well-rounded approach to cybersecurity risk. Such an approach must be supported by solid measures to prevent attack and to respond quickly and effectively should the worst happen.

Companies are not putting protective measures in place for their data as effectively as they could. A third of the survey respondents (34%) spend more money on marketing than on information security, and the numbers are not much better for sales and operations. Three in ten companies spend more money on human resources (HR) than they do on protecting their data, including their employee files.

Cybersecurity risks are much like any other threat to corporate wellbeing, in the sense that organizations have an opportunity to quantify it and respond accordingly. Assessing the risk and the potential impact enables them to allocate appropriate resources, preventing or at the very least mitigating the potential effects of an intrusion. More companies than ever before now understand the consequences if they fail to act.

Demographics

Vanson Bourne polled 1,000 business decision makers across seven countries in October/November 2015. It quizzed 200 each in the UK, US and Germany and another 100 each in France, Norway, Sweden and Switzerland. The majority (32%) came from financial services, banking and insurance, with the second highest proportion (14%) coming from retail, distribution, and transport. The remainder came from a variety of other sectors including computer services, wholesale, government and healthcare.

37% came from companies with 1,000 employees or fewer and 42% came from companies with between 1,000 and 5,000 employees, and the remainder came from companies with more than 5,000 workers.

Interviewees came from a variety of business-related functions, excluding IT, ranging from finance (the most popular at 19%) through to business direction and strategy (the second most popular at 14%). Functions including HR, engineering, marketing communications and legal were represented in the survey.

** Please note that due to rounding some charts may not add up to 100%.*

To learn more about NTT Com Security and our unique WideAngle services for information security and risk management, please speak to your account representative or visit: **http://www.nttcomsecurity.com/us/contact-us/** for regional contact information.

NTT Communications | NTT Com Security

We see a more secure world

NTT Com Security is in the business of information security and risk management. By choosing our WideAngle consulting, managed security and technology services, our customers are free to focus on business opportunities while we focus on managing risk.

The breadth of our Governance, Risk and Compliance (GRC) engagements, innovative managed security services and pragmatic technology implementations, means we can share a unique perspective with our customers – helping them to prioritize projects and drive standards. We want to give the right objective advice every time.

Our global approach is designed to drive out cost and complexity – recognizing the growing value of information security and risk management as a differentiator in high-performing businesses. Innovative and independent, NTT Com Security has offices spanning the Americas, Europe, and APAC (Asia Pacific) and is part of the NTT Group, owned by NTT (Nippon Telegraph and Telephone Corporation), one of the largest telecommunications companies in the world.