CYBER RESILIENCE

Cyber Resilience: bridging the business and technology divide

Stuart Rance

AXELOS.com

AXELOS GLOBAL BEST PRACTICE

White Paper

November 2014

Contents

1 CYBER RESILIENCE: BRIDGING THE BUSINESS AND TECHNOLOGY DIVIDE

Do you know how many security incidents your organization suffered from last year? If you think there weren't any then the chances are that you're in even worse trouble than people who can provide a detailed answer to that question. One cyber security firm recently estimated that as many as 71% of compromises go undetected[1].

Regardless of the size of your organization, the industry you operate in, or where in the world you're located, the chances are that you suffered at least one security incident last year, and the cost of these incidents is increasing.

As more and more aspects of our lives are digitized, and connected to the internet, the opportunities for attacks are increasing, the potential damage that the attacks could cause is increasing, and the need for us to prepare for these attacks becomes more urgent. This paper looks at how likely it is that your organization will suffer a security breach, how much that breach is likely to cost, and what you should be doing to protect your organization.

2 WHAT DOES THE DATA SHOW?

There have been a number of studies of the frequency and cost of different types of security incident.

Data from the UK[2] shows differences based on the size of the organization, but even small organizations were more likely than not to have had a security breach in the last year. See the following table.

Table 2.1: Security breaches in large and small organizations

	Large organizations	Small organizations
Percentage that had a security breach in the last year	81%	60%
Median number of security breaches in the last year	16	6
Average cost of the organization's worst security breach in the last year	£600K to £1.15m	£65k to £115k

One area of risk that organizations worry about is data breaches, where information that should be confidential is exposed by an attack. Data from a worldwide study[3] that looks at the cost and likelihood of different sizes of data breach shows the potential cost to organizations of this kind of incident.

The smallest breach considered in the study is 10,000 records, and the report shows that there is a 22% chance of an organization suffering a material data breach involving a minimum of 10,000 records within a two-year period.

The cost of a data breach varies depending on the country, ranging from $201 per record in Germany to $51 in India.

Multiplying these figures together shows that the smallest of data breaches (10,000 records) in the country where there would be the lowest financial impact ($51 per record) would cost more than $500,000. The average cost of individual data breaches in this report ranged from $5.85 million in the USA to $1.37 million in India. This is a huge impact for a risk that has a likelihood of 22% in two years.

3 WHO IS AFFECTED BY YOUR CYBER RESILIENCE DECISIONS?

A minor cyber incident might just be a small inconvenience to a few people within your organization, but if you suffer a major breach then it could affect lots of people. Not only would your staff and your organization be affected but it could have a major impact on your customers, your partners, entire supply chains that you are part of, and even on the infrastructure of the country.

Companies that suffer a major data breach may impact the privacy of millions of their customers. The effects on the business itself may be enormous. As well as direct costs, such as compensation and fines, the business may suffer considerable reputational damage, leading to significant loss of business in the short term as customers move away. Sometimes the brand is irreparably damaged. In the most extreme cases organizations may cease trading as a direct result of a cyber incident. For example, an attack on Code Spaces[4] deleted much of their customers' data and they were forced out of business. The National Cyber Security Alliance estimates that '60% of small businesses will close within six months of a cyberattack'[5]. Many organizations do survive cyber incidents, and many of these small businesses may have been about to fail anyway, but a well-managed organization should understand risks to their business, including cyber risks, and plan how they will respond to these.

Some organizations think that criminals are unlikely to target them as they have little of value to the attackers; they don't realize how these criminals work. If they can breach your company's security they may be able to use your systems or credentials as a conduit to your customers, potentially stealing much more lucrative information, and leaving your company with a lot of embarrassing (and potentially expensive) explaining to do. One well-publicised example of this was the major data breach at Target in the USA[6]. The hackers first breached a company that provided refrigeration services, and then used the refrigeration company's login credentials in the attack on Target.

As well as the cost and impact of a potential breach, you also need to consider the cost and impact of the controls you put in place to help protect your business and its customers. The cost of these controls includes not just how much you spend on implementing the controls, but also the impact they have on your ability to do business. Controls can affect both the efficiency of your own staff and how easy it is for customers to do business with you. If customers find your security controls too intrusive they may take their business elsewhere. If employees find your security controls too intrusive they may find ways to work around them, resulting in increased risk. Looking at this same issue from a more positive view, you may decide to accept a level of cyber risk in order to be first to market with a new innovation, or to make it easy for your customers to do business with you. What is important is that you understand the risks you are taking, and the benefits that you are hoping to achieve by taking those risks.

4 YOU CAN'T PREVENT CYBER INCIDENTS

However much you spend on cyber resilience, and however good your controls are, you can never completely defend your organization against cyber attacks. A sufficiently determined attacker will always be able to breach your controls and cause a cyber incident.

This doesn't mean that you should give up, and not bother to defend yourself at all. You can make it harder for the attackers, and a good set of preventative controls will defeat many attacks, resulting in a much lower frequency of security incidents. If you are very lucky you may be able to prevent significant attacks for an extended period of time, saving you cost and embarrassment. However, preventative controls can never be sufficient. You must recognize the likelihood that your security will eventually be breached and you need to have plans in place to deal with this.

As well as the preventative controls that you put in place to prevent attacks from succeeding, you need to invest in two other types of control:

- **Detective controls**, to identify when a security attack is happening. The sooner you detect an attack, the greater your ability to contain the damage and reduce the impact. Ideally, you should detect attacks before they have had a significant impact and take steps to prevent them from escalating. Many organizations have suffered data breaches that have gone on for months, because they were not detected, resulting in much greater cost than if they had been detected early. One of the most expensive data breaches in 2014 was at Home Depot, where malware that enabled criminals to copy credit card information from point of sales terminals was not detected from when it was installed in April 2014 until September 2014[7]

- **Corrective controls**, to correct the situation after an incident has been detected. There are many different types of corrective control, including a crisis management team, a security incident management process, a business continuity plan, and other pre-defined response plans for responding to known types of attack. These corrective controls can help to minimize the damage from a cyber attack, but they need to be well designed and properly rehearsed long before they are needed.

If your cyber resilience defences are mostly focussed on preventative controls then it is likely that you will eventually have a very expensive security breach. It is essential to invest in a balance of controls that prevent incidents, where it is cost-effective to do so, and also contain the damage from incidents that can't be prevented.

Your approach to cyber resilience needs to be built in to your management system. You can't just ask a security expert to create a set of controls while you continue to run everything the way you always have. You need to incorporate cyber resilience into the way you manage everything you do. One effective way to manage cyber resilience is to think about a cyber resilience management lifecycle. This approach is used in the forthcoming AXELOS Cyber Resilience Best Practice Guide[8], which describes a five-stage cyber resilience lifecycle based on the concepts behind the ITIL®[9] service lifecycle.

- **Strategy:** Understand your organizations objectives for cyber resilience, set your risk appetite, and define high-level policies

- **Design:** Design the management system and controls you need to meet the intention of the strategy

- **Transition:** Test all the controls and move them into operational use

- **Operation:** Operate your controls, detect and manage cyber resilience events and incidents

- **Continual improvement:** Ensure that cyber resilience continues to provide the level of protection you need in a constantly changing environment.

5 WHO'S ATTACKING YOU?

Many people think that cyber resilience is all about protecting the organization from gangs of cyber criminals. It is true that many of the biggest data breaches have been the result of attacks by criminals[3], but these are not the only causes of cyber incidents. Many attacks are carried out by insiders[10]; people that you have intentionally allowed access to your information. These insider attacks can be just as devastating as an attack by external criminal gangs. In March 2014, an insider published personal details of 100,000 employees of a UK supermarket[11], and the data that was exposed by Edward Snowden and Chelsea Manning has had a major impact on numerous governments.

Many data breaches are not attacks at all, but simply the result of carelessness or poor procedures. One example of this was the accidental loss of CDs containing details about child benefits for 25 million people in the UK[12]. This was not a malicious act, but it resulted in substantial embarrassment at the highest levels of government.

6 WHO IS RESPONSIBLE FOR CYBER RESILIENCE?

Cyber resilience is about more than just IT risks, it deals with business risks that could impact the survival of the whole organization. This means that decisions about cyber resilience need to be made by executive management and the board of directors (or equivalent).

Clearly, the board are not going to be experts in the technology aspects of cyber resilience, and nobody is suggesting that they should be. Design and implementation of cyber resilience controls will need to be delegated to people with specialist knowledge. Nevertheless, there are some aspects of cyber resilience where responsibility will always rest with the board. These include:

- Ownership of the risk to the business. The most significant risks to the business must be understood and discussed at board level. The board will be accountable to the shareholders (or equivalent in public sector organizations), and to regulators, for any major breaches. They must have sufficient awareness of the risks the business is taking so they can make the right decisions. The board should also decide on the overall approach to risk and the risk appetite of the organization, and they should communicate these clearly to people carrying out risk management. A summary of the risk approach is often shared with stakeholders via a company's annual report

- Budgeting for cyber resilience. There may be a need for significant investment to help the organization manage cyber resilience risks. People managing cyber resilience must be allocated sufficient budget to provide the agreed level of resilience

- Awareness and communication. One important aspect of cyber resilience is engaging staff, and ensuring that they understand both the risks, and their responsibility for helping to mitigate those risks. To be effective, this communication needs to have the support of the board, and be communicated top-down throughout the organization

- Crisis management. In the event of a major cyber incident, that could impact the future of the organization, the board will need to be briefed, and may need to make rapid decisions about how they want to respond. This can only be done well if crisis management responsibilities have been allocated, and people have rehearsed how they will respond to the various potential scenarios.

It is not only the board that has responsibility for cyber resilience. Everybody can make a difference to cyber resilience, either positively or negatively. Many security breaches can be prevented if people understand the risks and take appropriate actions, and the impact of security breaches can be minimized when everyone in the organization helps to detect and recover from the breaches that can't be prevented. Information security staff must ensure that appropriate controls have been designed and implemented. Information owners must understand their responsibilities for communicating the value of their information, and ensuring that it is properly protected. Technical staff must ensure that controls have been fully and correctly implemented. And everybody must help to identify and report risks, and must be vigilant to help defend against risks such as phishing attacks.

7 HOW SHOULD YOU MANAGE CYBER RESILIENCE?

Some organizations try to implement an information security management system, or a cyber resilience management system, which is independent of everything else they do. It has its own policies, procedures, standards, roles and responsibilities, goals and metrics. This kind of management system is often based on a standard such as ISO/IEC 27001[13] or the NIST Cybersecurity Framework[14].

There is a lot of value in following a standard, as this can help to ensure that you have comprehensive coverage of everything that needs to be included, but it is essential that you incorporate the requirements of the standard into your own management system. If you try to run cyber security as a completely separate activity to managing your business then there will be duplication and conflict, and you will not achieve your goals. It is also important that cyber resilience is managed in a way that meets the needs of the organization. For example when there is a major incident there may be a need for some business services to wait while others are restored. The decision on what the business priorities are for service restoration should be made by the business, not by cyber resilience staff or IT staff.

When you create the management system that runs your business, you define policies, procedures, standards, roles and responsibilities, goals and metrics. These should include everything needed for cyber resilience as well as everything needed for every other aspect of running your business.

Cyber resilience has a much wider scope than just IT systems and services, but the way you manage IT services can have a big impact on cyber resilience, so you will need effective IT service management (ITSM) to help achieve your cyber resilience goals. Adopting the ITIL best practice framework for IT service management[9] can help to ensure you have effective and consistent IT service management, and as explained above, the stages of the service lifecycle defined by ITIL can be equally useful in cyber resilience.

8 FIVE STEPS TO IMPROVE YOUR CYBER RESILIENCE

Every organization has some controls in place to provide cyber resilience, but we all need to make sure we continually improve. The people who want to defeat your controls are continually improving their skills and investing in new technology, your business is continually investing in new and improved technology, and their priorities are continually changing. If your cyber resilience doesn't also keep improving then it will gradually become less effective.

1. INCLUDE CYBER RESILIENCE IN REGULAR DISCUSSIONS AT BOARD LEVEL

Cyber resilience must be driven from the top. It is up to the board of directors (or equivalent) to set policy for how risk will be managed in the organization, to provide a suitable budget for cyber resilience, and to demonstrate their support for cyber resilience controls throughout the organization. This means that cyber resilience should be a regular topic at board meetings, with decisions about cyber resilience being documented and communicated throughout the organization.

Many major cyber resilience breaches can be traced back to a lack of leadership and governance, for example, before the Home Depot data breach, security staff had pointed out the need for new software and training, and managers replied “We sell hammers”[15], implying a complete lack of interest in cyber resilience.

Executive management should be involved in discussions about what information is critical to the business, what the risks to that information are, and what the high-level strategy for managing those risks will be. Summaries of this should be presented to the board for their agreement at regular intervals. This might be just once a year in a very stable organization or more frequently in an organization with more rapid change.

2. MAKE SURE YOU HAVE THE RIGHT BALANCE BETWEEN PREVENTATIVE, DETECTIVE AND CORRECTIVE CONTROLS

If you haven't reviewed your cyber resilience controls recently, then, it's likely that they are heavily biased towards prevention, with insufficient focus on detection and correction.

There are lots of things you can do to detect security incidents. Many of these involve using tools, which can be quite expensive, but there are open source tools that help you detect many types of attack (for example, to review log files, or create encrypted checksums for detecting unauthorized alterations to files).

Probably the most important corrective control that you need to focus on – if you haven't already done so – is the process you use for managing cyber incidents. When an incident happens, you need to respond quickly and correctly – to do this involves thinking through the likely scenarios and practicing how you would respond. Everybody who has a role to play needs to be involved in this practice, to ensure that they make the right decisions when they are under pressure from a real incident. Essential aspect of cyber resilience incident management include:

- Deciding who will manage the incident, and what resources will be available to support them
- Prioritising the need to investigate causes and protect evidence against the need to restore normal business operations
- Communicating the correct information to stakeholders. In addition to keeping staff and customers informed, this may include legal and regulatory requirements, as well as having a strategy for communicating with the press and shareholders
- Involving the right people with the skills and knowledge needed to resolve the incident
- Verifying that the incident has been resolved, and that no additional vulnerabilities have been introduced
- Learning from the incident to improve the incident management process, as well as reduce the likelihood or impact of any similar future incidents.

3. MAKE SURE YOU HAVE THE RIGHT BALANCE BETWEEN PEOPLE, PROCESS AND TECHNOLOGY CONTROLS

Many organizations focus their cyber resilience efforts on technology controls. Unless these are balanced with the right people and process controls they will be of very limited value.

Good cyber resilience depends on people with the right knowledge, attitudes, behaviour and culture doing the right things. If you don't motivate, train and periodically remind your people then your investments in security technology will be largely wasted. Similarly, if you don't have effective processes then the investment in technology will be wasted. For example, if you have invested in tools to detect when credit card data is being copied from your network, but have no process in place for responding to any alerts the tools generate you will get very little value from your investment. You only get the value if people understand that they must take the alerts seriously and have been trained in how to respond to them.

You need to provide your staff with appropriate training to ensure that they understand the need for cyber resilience, and the contribution that they can make to helping protect your business, but training is never sufficient, you also need to foster the attitudes, behaviour and culture that is needed. This requires senior management to consistently demonstrate the behaviours that they expect from others, as well as to issue regular reminders and encouragement.

Technology that is designed to protect your business needs to be configured and managed properly, and it must be reliably installed in every place that it is required. If a critical patch is missed from just one server, or a firewall rule is misconfigured on just one route, this can undermine all your investment in protective technology. Getting this right depends on the processes you have in place, and on the people who implement these. Processes that can help with this include, for example:

- Asset and configuration management to ensure that you know what technology you have to manage
- ITSM change management, to ensure that IT components are configured correctly before they are deployed
- Assurance testing and internal audit, to ensure that components remain in compliance with defined standards.

4. ADOPT STANDARDS AND BEST PRACTICES INTO YOUR MANAGEMENT SYSTEM

There are many different things that you need to do to provide an acceptable level of Cyber resilience. But if you try to design a management system to provide an appropriate level of protection from scratch, by simply thinking about what is needed, then you are highly likely to omit many essential controls.

Standards and best practices package the accumulated wisdom of many other people in a way that allows your business to incorporate the specific features you require within your own management system, to help ensure you cover everything you need. This enables you to learn from the mistakes of others, rather than having to make every mistake yourself.

You can’t simply adopt one standard or best practice to cover all of your needs, because they all have different scope and coverage and none of them is likely to provide everything you need to run your business. Some of the things that you should consider adopting into your management system include:

- AXELOS Cyber Resilience Best Practice Guide (to be published in 2015)[8]
- ISO/IEC 27001[9] – the international standard for information security management
- NIST Cybersecurity framework[10] – the US framework for improving critical infrastructure cybersecurity – this is also useful for organizations that don’t manage critical infrastructure
- ITIL best practice framework for IT service management[11] – the most widely adopted approach for management of IT services
- Management of Risk (M_o_R®)[16] – best practice framework for management of risk, to help organizations make informed decisions about the risks that affect their objectives

- ISO 31000 – International standard defining risk management principles and guidelines

- SANS Institute critical security controls[17] – a list of the top 20 recommended security controls. This can provide a great starting point for cyber resilience

- Cyber essentials scheme[18] – a UK government scheme to help organizations protect themselves against common cyber attacks.

5. KEEP UP TO DATE WITH EMERGING THREATS TO ENSURE THAT YOUR CYBER RESILIENCE CONTROLS REMAIN APPROPRIATE

Even if you design a perfect management system, and implement controls that cover every possible risk to your organization, this will still not provide you with all the protection you need. This is because threats to your cyber resilience are constantly evolving. Criminals determined to find ways of breaching organizations' cyber resilience devise new ways to attack, and vendors discover new vulnerabilities in their products. If you want to maintain your level of cyber resilience you must keep abreast of these evolving threats and vulnerabilities.

Make sure you are in touch with other organizations that operate in the same countries and industries as you, so that you can share information about new threats and vulnerabilities. You should also make sure you get updates from vendors of all technology that you use, to learn about new vulnerabilities and countermeasures from them.

Monitor publicly available sources of information such as US-CERT[19], CERT-UK[20], the NIST National Vulnerability Database[21], and lists maintained by private companies. These can help you to learn about emerging threats and vulnerabilities. Use this information to update your risk register, and regularly review your risk register to ensure you have correctly prioritized and communicated how you will respond to these threats and vulnerabilities.

ENDNOTES

1 Trustwave Holdings, 2014 Trustwave Global Security Report, May 2014

2 Department for Business Inovation & Skills, 2014 Information security breaches survey

3 Ponemon Institute, IBM 2014 Cost of Data Breach Study: Global Analysis

4 PC World, June 19 2014, Hacker puts ‘full redundancy’ code-hosting firm out of business

5 National Cyber Security Alliance, Small Business Online Security Infographic

6 Wall Street Journal, Feb 6 2014, Target Breach Began With Contractor’s Electronic Billing Link

7 Reuters, Sep 18 2014, Home Depot breach bigger than Target at 56 million cards

8 AXELOS Cyber Resilience Best Practice Guide, to be published 2015

9 AXELOS, 2011, ITIL Service Lifecycle Publication Suite

10 pwc, September 2014, Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015

11 BBC, 14 March 2014, Wm Morrison supermarket suffers payroll data theft

12 BBC, 25 June 2008, Timeline: Child benefits records loss

13 ISO 27001:2013 Information technology – Security techniques - Information security management systems - Requirements. Available from http://www.iso.org/, or from the standards organization in your local country

14 NIST Framework for Improving Critical Infrastructure Cybersecurity

15 New York Times, Sept 19 2014, Ex-Employees Say Home Depot Left Data Vulnerable

16 OGC, 2010, Management of Risk: Guidance for Practitioners

17 SANS Institute, Critical Security Controls - Version 5

18 Cyber essentials scheme, June 2014, Department for Business, Innovation & Skills

19 US-CERT United States Computer Emergency Readiness Team

20 CERT-UK United Kingdom Computer Emergency Readiness Team

21 NIST National Vulnerability Database

ABOUT THE AUTHOR

Stuart Rance is a consultant, trainer and author, and owner of Optimal Service Management Ltd. Stuart works with a wide variety of clients in many countries, helping them use ideas from IT service management and information security management to create business value for themselves and their customers. He is a Chartered Fellow of BCS (FBCS CITP), a Fellow in Service Management at prISM (FSM), and a Certified Information Systems Security Professional (CISSP).

Stuart shares his expertise widely, regularly presenting at events and writing books, white papers, blogs and pocked guides on all aspects of IT. He is the author of ITIL Service Transition, 2011 edition, and co-author of the ITIL V3 Glossary. He has written many pocket guides for itSMF, for the official ITIL portfolio and is one of the authors of the forthcoming Cyber Resilience Best Practice Guide.

REVIEWERS

AXELOS would like to thank Alex Hernandez (Director of CIO Advisory Services, KPMG US) for reviewing this paper.

ABOUT AXELOS

AXELOS are a joint venture company, created by the Cabinet Office on behalf of Her Majesty's Government in the United Kingdom and Capita plc to run the global best practice portfolio, including the ITIL and PRINCE2® professional standards.

The goals of AXELOS are many and varied, each one aimed at helping businesses and individuals reach success, empowering them to truly stand out in a competitive market.

- We continually promote and advocate quality training.
- We strive to encourage growth, development and progress.
- We always look for innovative new solutions to improve best practice standards and processes across the board.

The result is improved skills that are relevant to the industry as a whole, and enhanced employability for all, benefiting the global economy. The benefit to you and your business in particular: better trained employees, streamlined operations, and the peace of mind of knowing that you are working with an industry-leading organization, which provides products and services with a long-standing reputation for setting the industry benchmark.

ACKNOWLEDGEMENTS

Sourced and published on www.AXELOS.com.

Our White Paper series should not be taken as constituting advice of any sort and no liability is accepted for any loss resulting from use of or reliance on its content. While every effort is made to ensure the accuracy and reliability of the information, AXELOS cannot accept responsibility for errors, omissions or inaccuracies. Content, diagrams, logos, and jackets are correct at time of going to press but may be subject to change without notice.

TRADE MARKS AND STATEMENTS