Understanding Cyber Business Risk

An Introduction for Business Leaders

Technical White Paper

12 September 2014

OPENSKY
A TÜV Rheinland Company

Contents

Executive summary

The term cyber means different things to different people, but has certainly entered the vernacular in relation to computer hacking, data breaches and losses of huge amounts of customer information.

As businesses adopt an ever increasing online presence coupled with social media, e-commerce and smart devices, criminals and bad guys have realised there are richer pickings online than there ever where in the world of physical crime. Indeed we have a perfect storm of technology proliferation, intense economic pressures, a changed business environment and a younger generation coming to work with an “always on” mentality. All of these factors combine to create more opportunities for hackers.

This in turn leads to daily news articles telling of damaged corporate reputations and the personal woes of executives charged with sorting out the mess of a cyber-attack.

Key to understanding cyber business risk is knowing the basic measures that make up a strategy to deal with the problem. Governance is vital as it provides executive leadership to resolve the problem that is then assessed, measured and understood in relation to organisational objectives. A program can then be put in place to reduce cyber business risk making use of policies, technical controls and end user education.

This paper will help the reader understand the key elements of cyber business risk and how these may be addressed in their organisation. It will address the reality of the situation and provide a pathway for the reader to take action today, in their organisation, to reduce this risk.

The cost of cyber business risk failure

Protecting information assets is crucial if a business is to remain competitive and sustainable.

But every day we get news about data breaches, hacking, data loss and theft of intellectual property. It seems that the levels of aggressive hacking, state sponsored infiltration and insiders running off with sensitive data are increasing and little, if anything, can prevent it.

OpenSky believes that this is a strategic risk management issue for the business, and is better summarised using the term cyber business risk.

The cost of cyber business risk has been assessed in many studies over the years. The 2014 Information Security Breaches Survey [1], conducted on behalf of the United Kingdom government, revealed some startling statistics;

- £600k -£1.15m is the average cost to a large organisation of its worst security breach of the year
- £65k -£115k is the average cost to a small business of its worst security breach of the year

In the 2014 Cost of Data Breach Study: Global Analysis [2], written by the Ponemon Institute it was found that the average cost to a company of a data breach was USD $3.5 million, 15 percent more than what it cost last year

Clearly costs are rising.

Unmanaged cyber business risk can also have a catastrophic impact on a business and its leadership team [3];


Forbes

RETAIL 5/05/2014 @ 8:20AM | 26,677 views

Target CEO Gregg Steinhafel Resigns In Data Breach Fallout

+ Comment Now + Follow Comments

Clearly no executive wishes to be fired due to a data breach. A proactive management approach must be taken.

Benefits of managing cyber business risk

There are a number of benefits to adopting a proactive approach to cyber business risk;

- Corporates will be able to enjoy much better strategic decision making as cyber risk is factored into investment decisions and projects

- Improved decision making as a result of factoring cyber risk into investment decisions and projects will benefit the company strategically
- Financially the cost of data losses can be huge, both as the result of a regulatory fine and the expense of clearing up after an incident, so prevention and management of cyber business risk can have a direct financial saving
- Direct financial savings through the prevention and management of cyber business risk due to avoidance of regulatory fines and significant expense of clearing up after an incident
- Operationally the business is better prepared and conditioned for managing a cyber related incident
- Better preparation and conditioning for managing a cyber related incident

Once in hand cyber business risk can be managed to an acceptable level by most organisations.

But what of the detail?

Threat vs. vulnerability vs. risk

When discussing cyber business risk it's important to agree on some definitions and common language:

- Vulnerabilities are flaws or weaknesses that expose a system or process to compromise. A good example, familiar to many, is a vulnerability or flaw that is discovered in software which then needs to be patched with updated code
- A threat is the potential for a deliberate or accidental exploitation of a vulnerability. Not all threats are deliberate; for example the accidental loss of a laptop on a train can have as devastating impact as a deliberate hack of a web site.
- Risk can be defined as the potential of losing something of value. Every business and organisation faces risks ranging from the failure of a customer to pay an invoice through to the destruction of a factory during a fire. Executive leadership teams will spend a lot of their working hours evaluating risk against opportunities to grow and develop the business. Cyber business risk is another risk category to be assessed and understood and involves vulnerabilities and threats that relate to data processing, management and handling.

Having a clear understanding of these terms will help greatly in establishing an appropriate response to cyber business risk.

Quantifying cyber business risk

Accepting that almost all businesses or organisations use some form of information technology they also carry a concomitant level of cyber business risk. Crucial to managing cyber business risk is a need to understand the scope, scale and possible impact of a successful hack to an organisation. Only then can appropriate steps be taken to manage this

risk by applying controls – often in the form of governance, policies, technical equipment, processes and user education.

There are a range of formal methodologies that enable organisations to quantify their cyber business risk. Whilst suitable for many large organisations, for others the cost in terms of time and effort to conduct such assessments is often seen as prohibitive.

OpenSky supports a proportionate approach to cyber business risk and recommends that, whilst formal cyber business risk assessment programs have value, more tailored methods that synthesise best practices into a more palatable form may be more cost effective for many businesses.

For many organisations a cyber business risk review is better conducted as a combined risk and capability maturity review. By applying a capability maturity measure to each section under review, a baseline organisational cyber business risk review maturity rating can be obtained and used to demonstrate the value and progress of a remediation program to business leaders.

Governance

Effective information security governance is crucial to the success of cyber business risk activities as it demonstrates support and accountability from the leadership team. It also ensures that adequate resources, time and attention are given to this important area and that a culture of training and awareness runs through the organisation.

In many instances a cyber risk governance statement is created by the leadership team to clearly articulate the organisational position and support for this important area. This can be used to demonstrate such a commitment to customers and suppliers and build greater confidence in the management of this area.

Policies

Policies are the organisational rules that need to be followed when dealing with information or data assets. The tone, breadth and depth of these polices will often reflect the governance statement created by the leadership. Some heavily regulated businesses may have complex policies that cover many pages. In contrast, other businesses may have a lighter regulatory and policy requirement. For example, some may permit employees to bring their own consumer devices and connect them to corporate resources (often called BYOD or bring your own device); other businesses may explicitly ban this.

Policies are often created, owned and managed by a combination of the HR, legal and IT teams dependent on how the organisation is structured. Creating good policies that are understood and followed by users can be time consuming but that investment of effort will pay dividends as users will be less likely to push back, side step or ignore these important cyber risk controls.

Input from experienced legal advisors is most important as local, regional and national laws significantly impact what can and cannot be enforced in an information security policy. It is far too easy for an organisation to fall foul of employment laws and worker rights that will invalidate what was considered to be a reasonable requirement in a policy. The monitoring of users is an especially sensitive area as different jurisdictions will have different views on how often and precisely what can be monitored as a worker uses organisational IT systems. For example, the right to privacy often remains in place even if company email systems are being used for personal reasons.

Compliance and regulations

Every organisation is subject to cyber business risk related to regulations and compliance. These may apply only to specific sectors such as medical or financial, or have broader national or even international obligations. It is important for every organisation to understand the compliance and regulatory requirements that apply to themselves and determine how best to manage the various detailed requirements.

Confidentiality, integrity and availability

Known as the CIA triad, confidentiality, integrity and availability form the fundamental building blocks of cyber business risk management. Understanding cyber business risk in the context of this triad can help focus strategic thinking and associated investment.

- **Confidentiality** prevents sensitive data from being seen or accessed by the wrong people whilst ensuring that those that have legitimate need to access the data can do so. For example, identity and access management solutions enforce confidentiality and levels of data access often using a combination of passwords and user access rights.
- **Integrity** means ensuring that data remains accurate and consistent for its lifecycle. For example, it is vital to ensure the data integrity of an online transaction, preventing hackers from altering the amount of money being transferred whilst in transit.
- **Availability** refers to the importance of keeping computer systems online and accessible when required by the business. Denial of service (DoS) attacks are a common hacking technique used to overload computer resources so they are unavailable to legitimate users.

Most cyber business risk issues will fall into one of these categories, which make for easier understanding of why a particular technical control or process has been implemented.

Of course other information security properties need to be considered such as non-repudiation (the ability to prove data integrity and origin), authenticity, accountability, and reliability, but the CIA triad forms the foundation of this work.

Managing cyber business risk with technical controls

Inevitably some form of technology needs to brought to bear to reduce a particular set of risks.

The information security industry is vast, and there is no end of hardware and software products that can be purchased to address this risk but care needs to be taken that limited budgets are spent wisely.

Due to the relentless tide of new and innovative threats it is tempting to immediately address any cyber related problem with a piece of new technology or an upgrade. In fact, it is often the case that existing products and processes may be adequate for the level of risk being faced. Indeed it could be that a focused employee training session may be the best way to address a specific risk.

OpenSky believes that care needs to be taken in the selection of any technical controls and any expenditure needs to be proportionate to the risk the business faces. A lot can be achieved with targeted budgets.

The importance of end user education, awareness and training

Paramount in managing any cyber business risk is the need to inform, educate and coach users so they understand they are at the forefront of defending against threats. Many targeted attacks have been thwarted by smart employees detecting unusual activity and reporting it to the cyber security response team. This can only happen if users have been coached as to what to look out for as well as having the confidence to report such activity even if it subsequently turns out to be a false alarm.

Education is not a one off process and users need to be coached on a regular basis to keep their skills and awareness current and applied. Those on limited budgets need to ensure that end user education is addressed as a priority, and in some instances instead of an expensive technical control of limited longevity.

Future cyber challenges

Technology is evolving rapidly. Businesses need to embrace this change and develop new products, markets and solutions. Many now recognise the business value locked up in corporate data that needs to be mined and explored to discover insightful information on customers and business trends.

As internet enablement spreads, commodity equipment starts to become smarter and communicate information to control centres that may be located on the other side of the world. Cars, fridges, smartphones, home thermostats and microwave ovens start to form a connected domestic ecosystem. Industrial control systems in factories, smart transport systems on railway networks and supervisory systems in power stations start to talk across the internet using commoditised tools and protocols.

This “Internet of Things” presents hackers and malcontents with a whole new playground to research and launch attacks that will impact every business in today’s interconnected world.

OpenSky believes that addressing cyber business risk now is more vital that it has ever been.

Summary

Cyber risk is real, and a fact of modern life. The good news is that with a good understanding of that risk as it applies to an organisation, it is possible to put in place a proportionate response that balances the cost of remediation with the cost of something going wrong, thereby reducing the chances of the business being damaged.

What is crucial is that the problem is recognised and proactive action taken immediately.

Tomorrow may be too late.

Appendix 1 - Questions for the board

OpenSky believes that each and every leadership team should ask themselves some basic questions in order to understand cyber business risk as it applies to themselves;

- How confident are we that our company's critical information is safe and secure from cyber threats?
- What will be the impact to our share price, reputation, M+A activities or future success if our intellectual property or client data is lost or stolen?
- What would be the impact if our online systems were damaged or disrupted for a short or long period of time?
- Do we understand the specific risks that we face to our business and reasons why we may be targeted for our data?
- Is cyber business risk woven into our corporate risk register?
- What compliance, regulatory and legal frameworks must we adhere to and how can we reduce our exposure to legal action?
- Do we as a board lead by example in the way we value and protect our information assets to our colleagues, customers and suppliers?

Appendix 2 - Managing cyber business risk today

Distilling the complex task of managing cyber business risk into a few actions is difficult. That said, there are a few basic measures that each and every organisation can take to reduce their risk profile;

- Implement robust policies and procedures that are fully understood and embraced by users so they understand the important part they play in managing this risk
- Ensure all hardware and software is fully patched, kept up to date and is using the latest antimalware and antivirus signature files
- Deploy and manage end point encryption so that any lost or stolen computer equipment is better protected
- Have fully tested backup and disaster recovery plans so that lost data can be recovered in the event of failure
- Make sure that IT equipment is physically secure
- Have a policy and set of controls to manage mobile devices. These often contain the most current and sensitive corporate data available so need to be well protected
- Train all users to understand the importance of protecting organizational physical and data assets

About OpenSky

OpenSky Corporation provides information technology expertise to help corporations optimize IT platforms, protect information assets and accelerate the adoption of strategic technologies. We specialize in transformational IT infrastructure, security and compliance consulting.

We help enterprises with:

- Planning for IT optimization initiatives.
- Shifting computing to virtual and cloud based infrastructures.
- Developing next generation applications and data centres requiring next generation security and application security.
- Managing and securing the proliferation of BYOD and mobile devices.
- Mitigating risk and compliance across the organization.
- Developing highly functioning IT organizations while reducing costs.

OpenSky is distinguished from others by extensive technology expertise combined with deep industry experience. OpenSky specializes in Infrastructure; IT Risk Management and Security; Governance, Risk and Compliance; and Technical Business Consulting.

OpenSky has successfully delivered over 750 projects to Fortune 500 companies. Proven methodologies ensure a focused, consistent, project-based approach on every engagement. OpenSky maintains a business-centric perspective and believes that aligning premier technology partnerships with vendor-neutrality are critical and ensure the best solutions for clients.

TÜV Rheinland, is OpenSky's parent company and a $2B global leader in independent testing, inspection, certification, and consulting services. OpenSky believes that a highly experienced and qualified IT consultancy plays a valuable part in the design, optimization and security of IT and business.

References

[1] Annual data breach survey conducted by the UK Department for Business Innovation and Skills. Last accessed 7/8/14 http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

[2] Data breach survey undertaken by the Ponemon Institute. Last accessed 7/8/14 http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis)

[3] News report on Forbes website. Last accessed 7/8/14 http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/)