ResponSight

THE PRAGMATIC USE OF CYBER RISK AS A BUSINESS DECISION TOOL

September 2018

Author: Jeff Paine

ResponSight

ResponSight is a data science company focused on the challenge of enterprise Cybersecurity risk measurement over time, ranging in scope from single-endpoint to organization-wide risk. Our products employ state-of-the-art machine learning and artificial intelligence to develop detailed and accurate profiles of machines, departments, and enterprises.

While traditional systems actively search for known threats, ResponSight's approach focuses on learning user and machine activity. ResponSight performs analytics using activity metrics and statistical data to determine activity and behavioural fingerprints. Our solution responds rapidly to complex and potentially subtle changes in these fingerprints on a machine and across the enterprise, providing real-time visibility of risk to both security operations and executives.

Keywords: *cyber, cybersecurity, enterprise, risk, assessment, strategy, technology, data breaches, data protection.*

Introduction

As the number of cyberattacks continue to dramatically rise, today, it is even more crucial to have an effective cybersecurity strategy in place. Many companies are establishing formal security programs for the first time or seeking to optimise existing programs to improve the level of security maturity within their organisations. It is critical to create a security program that is pragmatic to your business environment and cyber risk profile. Traditional ways of thinking simply will not work.

Historically, the first piece of advice any business receives when it seeks out how it should best protect and minimise the impact of cyber security attacks has always been to invest in the latest security technology. Not only is it costly, but taking this outdated approach does not translate into the strongly held idea that the business is automatically shielded from threats.

Research from Accenture and Ponemon Institute [1] showed that cyber security breaches in Australia increased by more than 25 percent in 2017, despite Australian businesses increasing their security spending by 25 percent over their 2016 expenditures.

Enterprises continue to mistakenly choose technology as the first port of call to reduce their cyber risk. This is increasingly becoming more prominent among businesses in the Asia Pacific region when compared to North America [2].

However, what enterprises must understand is that their technology is not the solution to protecting their business, or reducing their cyber risk. Often, it serves as a way for them to distance themselves from being responsible for potential cyber risk.

Businesses need to move away from speaking to technology vendors as a first step in solving their security challenges. While vendors have long had a disproportionately high influence on business decision-making, businesses instead need start the conversation about business strategy by understanding their business cyber risk

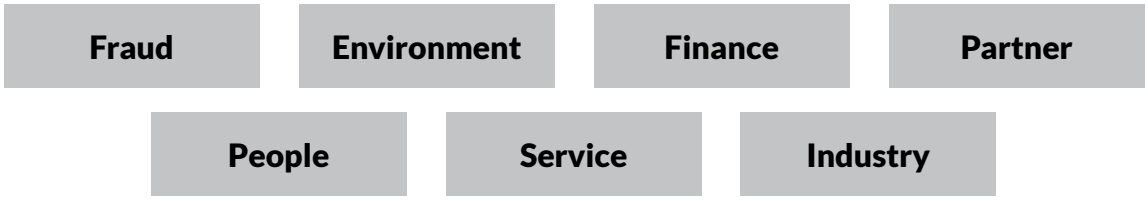
W: responsight.com **E:** info@responsight.com @responsight

How to assess your cyber risk

Risk assessments have traditionally been carried out against specific risk frameworks and standards, such as the factor analysis of information risk (FAIR) or through an information security management system (ISO). These usually involve self-assessed questionnaires and technical risk assessments that are essentially checklists to help examine the state of the technology and its configurations before an assessment is made on the "likelihood of a consequence matrix".

This means the responsibility often falls on one person to determine how vulnerable a system is, and if it is, what is the likelihood that cybercriminals will take advantage of it. The likelihood of that is always – not once but multiple times. This is why the traditional method of assessing cyber risk is a flawed approach - making assessing cyber risk in a pragmatic sense, impossible.

We need to move the needle towards using risk as an actionable tool by asking what's important to the business. This requires a business to determine which of the risks are the most important before knowing how to measure risk associated with those important tasks. These risks can be related to the following:



Once this information is determined, business can then make better decisions and set priorities, and use technology to assess dynamically the risks. This will be a step up from simply acknowledging there are vulnerabilities, use technology to address it, and then assume everything will be business as usual. This is a much more objective approach to assessing cyber risk, as it enables businesses to objectively manage risk in a repeatable and predictable way.

The regulatory influences on cyber risk assessments

A lot of the priorities around risk for listed or large proprietary companies are often driven by a compliance overlay determined by a regulatory body. For instance, the Australian Prudential Regulation Authority oversees the activities carried out by the Australia's financial services sector including their roles and responsibilities, frameworks, testing and internal audits, and information assets and controls [3].

The benchmark accountability for businesses to take control of their cyber risk is a lot higher now that new regulations such as the Notifiable Data Breaches scheme and the General Data Protection Regulation introduced in the European Union are now in place. This will help executives and boards frame conversations around the way they measure cyber risk and, more broadly, security. It will also enhance the awareness of cyber risk and bring forward the need for education on how to avoid falling victim to cyberattack.

Executives are now more encouraged to ask if what their business is doing is enough, and if the information is leaked when an attack occurs, what they should do. It will make businesses realise that their maturity level to deal with all the cyberattacks are not at an optimum level and at the moment they are delegating their responsibilities instead of dealing with the root cause.

As a result, companies have started to include cyber risk as a concern when assessing their overall enterprise risk management for insurance purposes. In turn, we have started to see the cyber risk insurance market grow significantly in the last few years. It is estimated the annual gross written premiums will grow to around $7.5 billion by the end of the decade .

Changing the cyber risk conversation

As the complexity of cyber risk management continues to evolve, practices for addressing cyber threats must change as well. This way, organisations are prepared to respond to cybersecurity events faster and more effectively.

Senior executives and boards are beginning to recognise cybersecurity as an issue critical to business performance, as opposed to an issue for IT to manage alone. Yet the gap between the information required for effective strategic decision making and the data provided by technology teams continues to widen.

> ***"The gap between the information required for effective strategic decision making and the data provided by technology teams continues to widen."***

Therefore, active involvement and oversight from the board is needed to ensure that an organisation is paying adequate attention to cyber risk management and decisions are based on business objectives. The board can help shape expectations for reporting on cyber threats, while also advocating for greater transparency and assurance around the effectiveness of the program. This reverses what has conventionally been a bottom up approach to cyber security management.

Boards and executives need to start asking their technology teams critical questions about the effectiveness of spending on IT security, a market that is expected to reach US$68 billion by the end of 2018 [5]. These questions include whether investing the enormous amounts of money on branded technology has changed the company's footprint, weakness, and exposure to cyberattacks, and how that is being measured.

The main reason boards and executives need to begin asking hard questions is because a common response chief technology officers and chief information officers give are often about how 99.7 percent of machines are protected. But board members are not technology people, so they will want to know about the remaining 0.03 percent – the same question that cybercriminals will also be asking, but for different intentions. This shows that while boards want to understand risk, technology people are not thinking about the same business objectives.

It is therefore imperative to change the conversation and mindset within technology departments. For a long time in Australia, IT reported to the chief financial officer, which is the root of why a lot of IT decisions are driven by cost, rather than business objectives.

Cyber risk, however, can be the common language that brings together business and technical stakeholders together in the context of setting business priorities. By leveraging information, boards can challenge management's assertions around the effectiveness of their cyber risk management programs, while also credibly communicating any related findings to other key stakeholders.

How the pragmatic use of cyber risk differs in business sizes

While the model of applying a pragmatic approach to cyber risk shouldn't differ between businesses – whether they're large or small – what does need to be considered is that the definition of risk may differ from business to business. A big risk for one business might not be the same for a second business.

If you're a small business and you don't have a good view on how to deal with risk then the damage could potentially be massive compared to a big business where something happening in one of their business units is of less concern and has less impact on the overall organisation. However, small businesses are far more nimble. They have a better grasp at setting priorities and have fewer stakeholders to appease.

On the contrary, it also means small businesses are at greater risk than larger businesses, mainly because they don't usually have enough resources. It also means they have to make very careful decisions on what technology they invest in.

Ultimately, regardless of the size of your business, you need to objectively, clinically and predictively manage and monitor risk over time. This way it gives the advantage of being able to proactively assess the risk of new trends, rather than reactively which has been a long-term trend when it comes to cyber risk.

"You need to objectively, clinically and predictively manage and monitor risk over time. This way it gives the advantage of being able to proactively assess the risk of new trends, rather than reactively which has been a long-term trend when it comes to cyber risk."

The future of risk measurement

With the number of cyberattacks rising and getting more sophisticated, cyber risk is ripe for innovation. Enterprises have realised traditional, subjective, point-in-time risk measurement and reliance on technology as the first port of call has limited influence on helping them make pragmatic business decisions.

At the same time, the accountability for businesses to take control of their cyber risk is now a lot higher with new regulations such as the Notifiable Data Breaches scheme requiring businesses to notify individuals when a data breach occurs.

Part of taking a pragmatic approach to cyber risk requires a change in conversation between boards and their technology team. We are starting to see a number of cases where there is now an improved relationship between the chief risk officer and chief information officer. The gap between business, risk, technology and vendors is closing. This way it ensures conversations are being driven from the top down, so the focus is more on business objectives, and less about technology and financial outcomes.

While the pragmatic use of cyber risk will differ between large and small businesses, it will ultimately provide businesses with a consistent scale for comparison and prioritisation, as well as greater clarity when it comes to setting strategic business priorities.

References

[1] Ponemon Institute LLC, "2017 Cost of Cyber Crime Study: Insights on the security investments that make a difference." Retrieved from https://www.accenture.com/au-en/insight-cost-of-cybercrime-2017

[2] International Data Corporation, "Worldwide Spending on Security Technology Forecast to Reach $81.7 Billion in 2017, According to New IDC Spending Guide." Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS42425417

[3] Australian Prudential Regulation Authority (APRA), "Discussion Paper, Information security management: a new cross-industry prudential standard." Retrieved from https://www.apra.gov.au/sites/default/files/20180307-Discussion-Paper-Information-Security-Management.pdf

[4] PWC, "Insurance 2020 & beyond: Reaping the dividends of cyber resilience." Retrieved from https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html

[5] S. Sarraf, ARN, "Global security spending to reach US$96B in 2018." Retrieved from https://www.arnnet.com.au/article/631021/global-security-spending-reach-us-96b-2018/

For further information visit www.responsight.com