Key Security Challenges

Abstract

Information security breaches are a major business problem, the consequences of which can seriously erode consumer confidence and wipe millions off a brand's value. In the wake of the growing sophistication of cyber adversaries, the unprecedented volume of attacks and increasingly harmful IT security threats, coupled with stricter regulatory mandates, the need for organisations to be on top of information and cyber-security is greater than ever.

This paper explores a number of key challenges that organisations are facing today in managing their information and cyber security.

Information Security Challenges

Businesses are facing unprecedented levels of risk associated with threats to their information assets. Barely a day goes by without hearing a report of a new data breach, cyber-attack or phishing campaign. The threat landscape has clearly evolved, with new threats emerging all the time that threaten the security of organisations around the world. There's little doubt that cybercrime will continue to dominate the headlines for years to come. As cybercriminals become more sophisticated and devious in their attack methods, organisations will need to ensure they have robust systems in place to defend against these evolving threats.

Whilst business has little influence over the information security risks they face in conducting their business activities and even less influence over cyber criminality they do have complete control over how they manage and protect their information assets. However, it is abundantly clear that a large number of businesses need significant help in this exercise. The accelerating pace of technology advances together with an insatiable appetite from consumers is driving many businesses into areas that they are ill-prepared to operate in.

Managing security is an ongoing process that evolves and changes over time in line with the ever-changing threat model. Businesses are subject to increasing and ongoing demands to compete which mandates agility and flexibility to adapt at short order. These demands are exacerbated with pressures to also provide services or products at more competitive price points. The effective enforcement of security can only ever be based upon structure, consistency and rigour all of which are not necessarily easily aligned with business and technology operations staff often struggling to keep the lights on.

Research carried out by Verizon & Ponemon has clearly identified 5 key threats facing businesses today:

- Inconsistent application of basic security controls
- Lack of meaningful and actionable information to support decision making process
- Failure of IT & business teams to collaborate
- Reliance on manual processes to manage security
- Shortage of skilled resources across IT and the business to support InfoSec

The following sections explore these challenges in more detail

Inconsistent application of the basics

The myriad of configuration options within an IT infrastructure are all potential vulnerabilities if mis-configured and exposed. Unfortunately, it is all too easy for these vulnerabilities to be introduced and as a consequence of being exposed then be exploited. The inconsistent application of security controls is a major threat to business as borne out by the Verizon Risk Report that identifies 98.5% of security incidents can be categorised into one of nine patterns, and 75% can be categorised into one of three patterns.

Consistency across the IT landscape is a huge problem for many organisations, especially those with large and complex environments. This lack of consistency can be considered highly damaging to the security posture of

an organisation and its capacity to adapt to change which in turn places the overall business at risk. Without consistency the notion of enforcing security remains purely academic. There are many factors that lead to inconsistency, as an example mergers and outsourcing of business units. The complexity involved in delivering an outsourcing program or a merger is generally detrimental to enforcing consistency across the infrastructure.

If achieving consistency is a monumental task for a lot of organisations then maintaining it is nothing short of miraculous, especially given the amount of change that occurs within their environments. The constant churn inherent in many infrastructures means that just supporting the environment takes all the time and energy available and ensuring consistency remains a luxury that is out of reach.

An example should help clarify things:

> *Strong security goes hand in hand with consistency. When you lock your house up for your annual vacation you go through each room in turn making sure that all the windows and doors are locked, and the burglar alarm is set. What you are doing is nothing short of executing a process. The larger the house the more time you spend on the process. Even though this is a slightly trivial example it illustrates the need for process and discipline to make sure the likelihood of getting burgled is minimised. It is only through the rigorous adherence to the process that consistency is achieved – in our example all entrances and ways into the house are secured. A more haphazard approach may have missed the closet window because the closet is hardly ever used, which would have resulted in the whole security of the house being undermined through a simple lack of consistency.*

At the fundamental level Security Management when applied to an IT infrastructure (or business as a whole) is doing nothing more than ensuring that all vulnerabilities are addressed and locked down wherever possible. This is analogous to securing all the entry points into the house in our example. However, as there are significantly more variables and things to lock down in an IT infrastructure than in an ordinary house the level of complexity is much greater and as a result many areas are not adequately addressed and so we get inconsistency.

The opportunity for inconsistency is rife across all areas of IT infrastructures and can be considered a risk whatever form it takes – i.e. patchy monitoring of routers and switches may not on the face of it pose a security risk, though a problem with a router that is not being monitored may well result in a loss of service which is exactly one of the areas that Security Management is trying to protect against.

Visibility

Most business leaders would struggle to articulate their organisation's Information Security Posture – i.e. how well they protect their information assets and how well they would re-act to a security incident. Furthermore, they would probably be shocked to understand the risks to which their businesses are exposed to on a daily basis. Even companies with large IT security organizations do not manage their security risks well because the information provided to senior managers and the Board is not meaningful (typically too little or too much) and does not provide a basis for action.

The old adage of "if you can't measure it, you can't improve it" is particularly apt in the case of managing information security. Without up to date business-level visibility of an organisation's entire Information Security Posture it is unrealistic to expect senior management to understand where gaps and weaknesses exist that threaten the organisation.

One of the original aims of GRC (Governance, Risk Management and Compliance) was to provide better visibility into a company's risk posture and thus enable improved decision making. Ten years on from the birth of the GRC software industry it is perhaps ironic that the failure of many GRC projects is due to a disconnect from risk – GRC oriented risk programs tend to focus on compliance objectives to the detriment of risk and of course compliance to any standard does not necessarily remove any risk. Businesses that have embarked upon GRC projects have however definitely benefited from an increase in maturity across both Cybersecurity and operational resilience even if they have not achieved the visibility to allow them to make better decisions.

Measuring the effectiveness of an organisation's Information Security Management program must include an assessment of the technology used to support the business information assets if it is to be considered accurate and representative. The reconciliation of security instrumentation implemented across an organisation's technology environment is the only conclusive proof that security policy is being correctly enforced – i.e. the Acid Test. Extending this even further, a fully representative understanding of an organisation's security posture would include attestation across all parts of the organisation to testify that security policy was indeed compliant. Tracking all security controls across an organisation would in theory provide a complete dataset upon which a comprehensive information security posture could be derived

Collaboration

Managing the security of an organisation's IT infrastructure requires a deep technical understanding of the IT environment and how security controls are administered and managed, while at the same time ensuring satisfactory levels of system performance and availability. This dependence for understanding is usually far outside the remit of a business executive whose main focus is on executing and maintaining business strategy and managing business performance against shareholder expectations. Indeed, articulating the challenges to business has been particularly poorly executed by IT.

Consequently, this has resulted in a "gap" in understanding, communication and collaboration between business executives and the IT division and/or those in the business looking to exploit technological innovation by deploying new IT solutions to support business growth demands (ref. "Shadow IT", IoT, etc.). Businesses are under pressure to transform and evolve around changing business models in sympathy with new consumer markets and behaviours. The correct and timely deployment of new technologies in alignment with the needs of the business, are critical to modern business growth strategies. But if business-leaders are unable to proactively manage and maintain effective & business-aligned Risk Management and Information Security Management strategies, the organisation will always be at risk of failing in its duties and obligations to its shareholders.

Finding a solution of bridging the "gap" from an Information Security Management perspective should therefore be a critical issue. Over the last few years, the recognition of the problem has become more prominent, although the problem still largely prevails. The complexity of finding a solution to the "gap" problem can be likened to two

groups trying to communicate but not understanding each other. Business executives will rarely excel in their understanding and appreciation of technology and IT disciplines. Likewise, IT and technology staff are not expected to understand everything about corporate strategy, financial and risk management, corporate governance, etc. So, if this status-quo cannot change, the solution to the problem cannot be one of filling the gap, but one of building a bridge across the gap. A bridge of "effective understanding, communication and collaboration".

The major stumbling-block to realising an effective security culture throughout any organisation, is that the drive to achieve this must be business-led - senior business and technology leaders, must themselves have a consistent and persistent alignment of understanding of what is involved in developing and maintaining an effective information and cyber-security posture.

Manual Processes

Managing an IT infrastructure is in general a complex undertaking. This complexity is exacerbated when scale and heterogeneity are introduced. The management of large and heterogeneous infrastructures is therefore only realistically possible with the use of tools and the adoption of robust methodologies and practices. In fact, I would argue that without well-structured methodologies like ITSM & ITOM it would be impossible to manage any technology infrastructure (even relatively modest ones) with any confidence.

However, the management of Information & Cyber Security is for the most part performed using manual processes and spreadsheets. Tracking of security controls, risks and other security related activities is typically recorded in spreadsheets by humans. Scheduling of repeatable tasks is achieved through personnel calendar entries. This is surely ironic. We are all aware of the human frailties associated with performing mundane and repetitive tasks – the benefits of automating those tasks with computers is well understood, yet the critical management of Information & Cyber Security is still managed manually.

In the "2019 State of the Firewall" report, Firemon clearly identify network security risk at an all time high. One of the major reasons for this is the reliance on manual processes when it comes to configuring network devices and managing change processes leading to costly misconfiguration errors. Abstracting these findings across the whole of the IT environment it is clear that the dependency on manual tasks and growing complexity of technology implementations is a recipe for disaster.

Skills Shortage

The skills shortage prevalent in Cybersecurity is nothing new. It's a problem that business has been facing for several years now and it's only getting worse. There are a lot of reasons why the gap is widening, a few are listed below:

- IT solutions are still developing, and more organisations are adopting IT across more and more areas
- Criminals continue to find new ways to exploit IT vulnerabilities.

- When businesses grow, so does the complexity of their systems. This means that not only are there more assets to protect but they are more difficult to protect.
- Cybersecurity courses have not yet been adopted by enough educational institutions

Furthermore, Cybersecurity skills are not always easy to learn. Not only is a good understanding of IT required but for more senior roles extensive skill sets including development and administration as well as an inquisitive and creative mind and the ability to think outside the box. These exacting criteria naturally limit the talent pool.

Conclusions

Information Security Management can only ever be effective when performed in an ordered manner - i.e. through the adoption of structure, consistency, accountability, and rigour. This approach results in a repeatable and predictable security domain enabling business to move forward with confidence. Inconsistency in whatever form it takes poses a significant risk to business as is evident by the widespread exploitation of basic vulnerabilities that would have been addressed had the application of basic security controls been performed.

The lack of visibility into an organisation's Information Security Posture is extensive across all business. This in itself needs to be considered a significant risk - CISOs and business leaders are in effect operating blind, with the downsides to making a wrong decision or no decision at all often being disastrous. Senior management need up to date and contextual information now if they are to stand any chance of navigating their businesses through these troubled waters.

The relentless evolution of technology and its adoption into more and more areas of business and general day to day life brings with it not only progress but also the opportunity for new and more exotic vulnerabilities some of which we can't even yet imagine. One thing though that is known is that the current reliance on manual processes to manage security is unsustainable. The ongoing shortage of skilled resources is only exacerbating the demise of this manual dependency. We are already seeing the uptake of SOAR (Security, Orchestration, Automation & Response) solutions that enable businesses to respond to low level security events without human assistance. The next logical step is to transition this automation from purely re-active scenarios into pro-active scenarios facilitating the delivery of continuous compliance and identification and remediation of exposures before they are exploited.

THE END