Chartered Institute of Information Security

Pulse:

November 2022

CIISEC LIVE 2022

We finally made it to the Craiglockhart Campus in Edinburgh

CIISEC INNOVATION SUMMIT 2022

Themes included Cloud, Supplier Management, Human Behaviours

RANSOMWARE

The subject that cyber professionals can't seem to get away from

The Threat Landscape

The year 2021 was marked as another continuing period where cyberattacks were more prevalent due to the Covid-19 Pandemic and many other conducive factors where cyber actors sought to disrupt and seek financial gains from compromising and breaching businesses and organisations.

Edward Millington (BSc, CISSP, ISSA, MCIIS, MIET, PAN-ACE) Founder & Managing Director of CariSec Global Inc.

Leading this trend and in many cases, taking the top two positions globally on the threat landscape scale is the Ransomware cyber-attack.

Ransomware, as highlighted by various global threat reports , continues to increase year after year and as previously mentioned, dominates many other types of cyberattacks where cybercriminals are demanding greater and greater sums of money and more often than one would expect, receiving part thereof. One can consider such scenarios as the leading driver behind this type of attack and with the advent of cyber-insurance and its coverage, it is believed that this has spurred such attacks to greater levels. Such cyber-attacks increase cyber risks to sectoral businesses tremendously - as it is financially driven and preys on the security operations vulnerabilities of businesses and organisations - irrespective of operational risks losses they can cause. While such reports alert business sectors of the growing Cyber Threat, overall operational risks continue to surmount where attacks by threat actors not only cost businesses millions of dollars per year but more critically the clients' privacy, identity, and possibly safety; and in 2022 – the current year, this trend is expected to worsen, affecting many businesses at varying economic levels, while dominating headlines in major corners of the globe, as businesses are required to report breaches due to data protection laws.

Threat Landscape:

The Threat Landscape, previously mentioned, continues to advance as businesses evolve to meet Digital Transformation requirements and demands, where in today's society the access to information, services, and transactional operations is expected to be carried out immediately, at any time, and anywhere in the digital space; instantly at finger-tips. This necessity has driven the increase of technology, process, and people across a range of technologies, geographical locations, geopolitics, and cultures, thereby leading to the expansion of Attack Surfaces of the business to cyber threats - increasing qualitatively and quantitatively cyber risks to the business. To further highlight this grave issue, cyber risks continue to grow to double-digit rates every year for businesses (highlighted by global threat reports), which seems to be not well understood for risk management, since there are ever-increasing incidents and breaches where greater attack surfaces are not only affected but large amounts of data is encrypted and exfiltrated, and in most recent times, threatened to be released to shame the business if no ransom is paid. The character of the cybercriminal (ransomware attacker) is ever-evolving for extortion and business leaders must be aware of this to respond strategically.

Reasserting, as a business' digital footprint expands, so do its attack surfaces and its threat landscape. The core focus of any business is to be financially viable and market competitive for its shareholders in the delivery of goods and services based on strict timelines, goals, and or market expectations and in so doing, may not carry out the due diligence in the application of Enterprise Security (unless adhering to regulations, standards, etc.) at a high maturity level. The ability to operate at high-security levels implies that the Enterprise Risk Management program is also operating at the same level or greater, implementing and monitoring risk-based Security Controls through the Information Security Governance Program, for their effectiveness, efficiency, and application, thereby resulting in the reduction of risks and attack surfaces and in essence, improving cyber resilience and business trust. But this is not always the case where Cybersecurity & IT Risk Management (all activities of a risk-based Information Security Governance Program) may be a part of the Enterprise Risk Management program and therefore may not be very well developed to risk treat the evolution of cyber threats.

An Information Security Governance Program is a guiding document that strategically aligns the organization, its people, process, and technology to the organization's vision, goals and objectives; through security frameworks, policies, standards, procedures, and guidelines in securing business assets.

The ability to operate at high-security levels implies that the Enterprise Risk Management program is also operating at the same level or greater, implementing and monitoring risk-based Security Controls through the Information Security Governance Program, for their effectiveness, efficiency, and application, thereby resulting in the reduction of risks and attack surfaces and in essence, improving cyber resilience and business trust.

Security Maturity:

Security Maturity Model Levels:

The proliferation of ransomware implies that cybercriminals are taking advantage of the Information Security Governance Program's wavering operating maturity to exploit the threat landscape for further financial gain, and or to cause serious to critical operational risks.

The maturity of an Information Security Governance Program is affected by:

- The C-Suite inability to understand and support organization-wide cybersecurity strategies governing security at all levels throughout the organisation.
- The inadequacy of Cyber Threat Intelligence (CTI) used in the Risk Management Program where cyber risks can be treated appropriately with respect to the business' risk tolerance. The inadequacy provides an unclear picture of the threat landscape for risk management.
- Risk management activities and processes are not carried out well due to the lack of resources and or inexperience of risk consultants.
- Human resources lacking critical IT & cybersecurity skills and or the professionalism to carry out their jobs.
- All stakeholders, who will be supporting the program, lack the understanding that such a program must have a lifecycle for effective program activities in supporting the organisation's mission, business strategies, and goals.

The proliferation of ransomware implies that cybercriminals are taking advantage of the Information Security Governance Program's wavering operating maturity to exploit the threat landscape for further financial gain, and or to cause serious to critical operational risks.

An underdeveloped Information Security Governance Program will have the following consequences on the security maturity of a business/organisation:

- Critical Risk-based security policies are underdeveloped or not enforced, leading to ineffective, inefficient, and insufficient security controls.
- Monitoring of risk-based security controls is inadequate, which may lead to security controls becoming non-compliant, thereby making them inefficient or ineffective.
- Procurement process not security-aware enough in the acquisition of solutions and services.
- Program activities in relation to risk-based security awareness and practices are underfunded.
- Change Management activities and processes are not guided and carried out effectively and efficiently due to underdeveloped change management policies.
- Third Party Policies are poorly constructed for Third-Party Risk Management (TPRM).
- Cybersecurity awareness training programs are inadequate.
- Security controls in the identification, protection, detection, response, and recovery of cyber threats are inadequate, affecting cyber resilience.
- Incident Management activities and processes to respond to incidents are either inappropriate, ineffective and or inefficient, affecting cyber resilience.
- Backup Continuity and Disaster Recovery Planning policies in the response to a critical service and or operational incident are underdeveloped, affecting business resilience.

CONCLUSION

To achieve high levels of security where cyber risks are managed effectively and efficiently in the operations of the business, the Information Security Governance Program must not only exist but must also be Risk-based matured, and seen as an integral part of the operations of the organization/business – from top to bottom.

Therefore, until information security governance programs can be operated at a high maturity level in the protection of assets, the ability to manage cyber risks posed by the threat landscape in which the business/organization operates will always be vulnerable to ransomware attacks – a process that is always used to extort financial gains by cyber-criminals due to weak cybersecurity postures and spurred by the willingness to pay the ransom (and in many instances, covered by cyber-insurance) all in hast to return business operations quickly for business continuity. The rush to return the business back into operations could also lead to further future attacks if security lessons are not learned and shared among the sector(s).

About The Chartered Institute of Information Security

The Chartered Institute of Information Security (CIISec) is the only pure play information security institution to have been granted Royal Charter status and is dedicated to raising the standard of professionalism in information security.

CIISec provide a universally accepted focal point for the information cyber security profession, it is an independent not-for-profi t body governed by its members, ensuring standards of professionalism for training, qualifi cations, operating practices and individuals. CIISec has a growing membership that represents over 10,000 individuals in the information security industry.

Evesham Office
Haddonsacre
Station Road
Offenham
WR11 8JJ

www.ciisec.org

Chartered Institute of Information Security