(ISC)² Spotlight

Cyber Risk Management Strategies – A CISOs Perspective

Andy Smeaton – CISO, Afiniti
Greg Rogers – CISO, LGA

Presenter Bios

Andrew is a globally experienced certified Information Security executive and Board Advisor with over 26 years of experience in the banking, financial services, startups, and healthcare industries. His experience ranges from building information security teams from the ground up, enabling sales as a customer-facing CISO, maturing systems to reduce risk, and developing streamlined reporting to provide executive insight into data risks.

Andrew has been a recent keynote speaker at InfoSec World 2022, SecureWorld Boston 2023, was awarded the (ISC)² CEO Award of the year for 2022, and is well known for his excursion into Ukraine to rescue a colleague and his family.

Greg is a cybersecurity leader with over 20 years of broad IT and security experience. He spent 15 years of his career as a contractor in the Dept. of Defense specializing in communications security, encryption devices, and cyber risk management of mission critical systems. More recently Greg has served as the CISO of a US financial services company, where he has focused on building a mature information security program from the ground up, managing cyber risk in alignment with business functions, and achieving regulatory compliance.

Learning Objectives

Join us as we examine enterprise cyber risk management strategies. We will discuss our views on different risk management approaches for different types and sizes of organizations and will provide some of our own real-world experiences.

Information security is like the brakes on a car, it keeps the business from going too fast and crashing. Frameworks tell you what components the braking system **should** have, and regulations tell you what components it **must** have. Risk-Aware Decision Making helps you design the system to acceptable tolerances.

Understand

- Understand why and how risk-aware decision making is critical for a balanced cyber risk management strategy.

Learn

- Learn how to select security frameworks (such as NIST, ISO, and CIS) most appropriate to your specific organization.

Gain

- Gain insights on the necessity of a written information security program, and the reality of approving security exceptions.

Standards & Frameworks

Written Information Security Program

- Benefits of a written information security program include standardization & formalization, which improve implementation and adaptation & updating.
- This includes policies, standards, and guidelines, as well as documented processes and procedures.
- Standardize exception request & approval process, document approve / deny decisions.
- Develop a formal Risk Acceptance process.

Don’t “do business with out knowing how you do business”.

Information Security Frameworks

- Framework Examples: NIST CSF, ISO 27001, CIS v8, COBIT, CMMC, HITRUST.
- Frameworks help guide development of security controls and processes.
- Improve standardization and maintenance of a security program.
- Help prevent omission of key security requirements.
- Assists development of roles and responsibilities for security and IT staff.

Don’t be “successful by accident”.

Regulations & Risk

Regulations Impact on Security Program

- Regulations impact security and risk management strategies.
- May required controls that don't effectively or measurably reduce risk, or that may negatively impact business functions.
- Regulations are mandatory, based on industry sector, services offered, and clients.
- Regulatory Examples: NYDFS 23/500, SEC/FFIEC, SOX, HIPAA, PCI-DSS*, CCPA, GDPR, FedRAMP, NAIC IDSA.
- *PCI-DSS is an industry contractually enforced security standard.*

Cyber Risk and Business Requirements

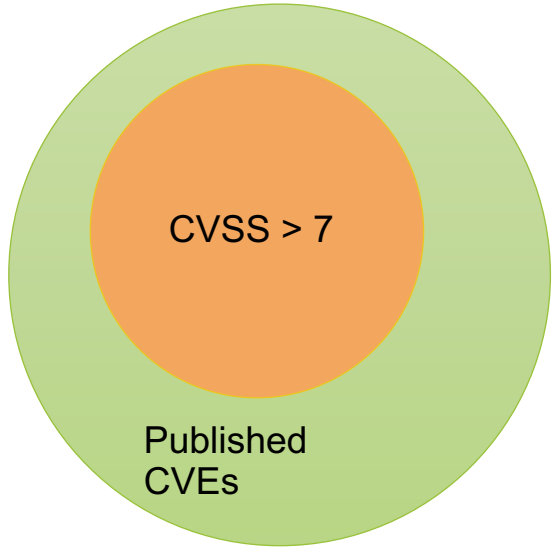
- Balance between cyber risk and business operational requirements.
- May need to omit or tailor specific controls to support business requirements.
- May need to replace technical preventive controls with detective or procedural controls.
- Perform and use your cyber risk assessment.
- Weigh the security risk vs. business reward.
- Reality of security exceptions & compensating controls

Vulnerability Management

Vulnerability Severity

Prioritize vulnerabilities based on their severity and impact on information systems.

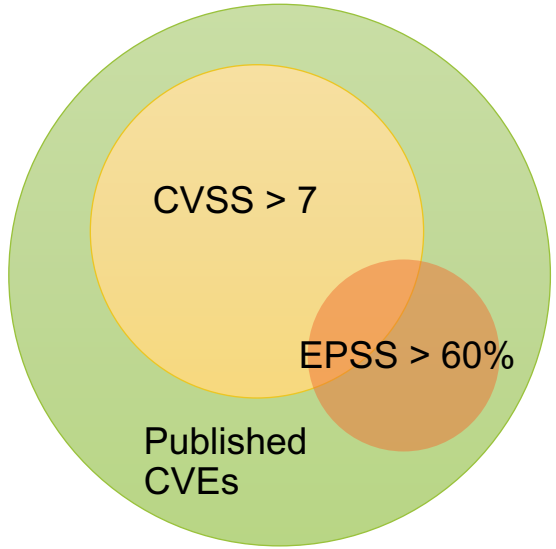
Common Vulnerability Scoring System (CVSS) – Rates vulnerabilities based on their severity. Provides a score from 0 to 10, with higher scores indicating more severe vulnerabilities. Implemented as intended it takes into account factors such as exploitability, impact, and affected assets; *but this is often skipped due to high level of effort and limited time to assess*.



Vulnerability Exploitability

Prioritize vulnerabilities based on their likelihood of being exploited in the wild.

Exploit Prediction Scoring System (EPSS) – Considers the probability of a vulnerability being exploited in the wild. Provides a score from 0 to 100, indicating the likelihood of exploitation. Research has shown firms are able to fix 5%-20% of known vulnerabilities per month. Only a small subset (2%-7%) of published vulnerabilities are ever seen to be exploited in the wild.



Other Strategies

Location-based involves prioritizations based on accessibility to information assets to attacks and malware, such as internal servers vs. end user systems.

Asset-based involves prioritizing vulnerabilities based on the importance of the asset or system, such as critical systems or those that store sensitive data

Myth of the Advanced Attacker

Most breaches are exploits of poor basic cyber hygiene. Poor monitoring and detection results in long dwell time. Infrequent assessments and log reviews are other contributing factors.

Examples include unpatched systems, weak passwords, lack of anti-malware, lack of usable backups, social engineering, lack of MFA, email compromise.

Don’t fall victim to the next shiny thing or marketing buzzword. Strong cyber hygiene and education will mitigate the majority of attacks. Focus on your chosen framework, regulations, and risks.

Risk-Aware Decision Making

The ability to make risk-aware decisions is critical for effective cybersecurity leaders to balance cyber risk against business functions. The focus is on **accepting risk** to **support business** operational requirements. This technique can be applied to all types of business decision making.

Goals

- Acceptable Risk Level
- Maintaining Regulatory Compliance
- Enabling the Business
- Building Awareness of Organizational Risks
- Implementing Controls with Least Friction
- Maintaining Compliance with Enterprise Polices & Standards

Benefits

- Make informed decisions about cybersecurity requirements, controls, and business processes.
- Guides organizations in effectively and efficiently allocating financial and personnel resources.
- Helps organizations identify potential threats and their probable impacts before they cause harm.
- Enables stakeholders to focus on areas/threats of greatest risk to the organization and key functions.

Risk-Aware Decision Making

There are several factors to consider in decision making. These factors combine cyber risks, regulatory mandates, and business needs to achieve the best outcome and effective risk mitigation for the organization.

Factors for Consideration

- **Risk Tolerance:** financial, operational/downtime, reputational, regulatory.
- **Regulatory & Contractual Requirements:** what controls are optional vs. mandatory?
- **Asset Value & Budget Constraints:** control & mitigation cost vs. asset & business cost.
- **Threat Likelihood & Impact Severity:** how likely is a significant impact from an attack?
- **Resource Availability:** time and materials cost, opportunity cost.
- **Business Impact:** loss of productivity, loss of sales, loss of partnerships, loss of customers.

Data Driven Risk Management

Metrics can be used to drive your risk management program. A mix of Security and IT metrics is required, as security metrics alone don't convey the information required to make risk decisions. Don't use metrics that don't directly help you determine effectiveness or compliance of you information security program, or that don't help you identify areas for risk mitigation. Your metrics should also relate to your key business functions and business risks.

Security & IT Metrics Should:

- Have value to your program and business.
- Be based on your regulations, framework, business requirements, risk assessment.
- Support your risk-based decision making, as well as measure security program compliance.
- IT metrics should be relatable to your security metrics and help them provide context to your systems.

Metrics Do's & Don'ts

Don't just list numbers of open vulns, unpatched systems, missing AV/agents, stale accounts, open pen test results.

Do provide information about characteristics of assets (network location, classification of data, business process supported), access level, and exploitable vulnerabilities/security gaps.

Number of open issues correlated to number of IT assets can provide quick view into level of compliance.