Unit-4 (1): Security Governance and Management

Incident Management and Response Metrics

INCIDENT MANAGEMENT DECISION SUPPORT METRICS

What Kind of Incident Is It?

There are generally few metrics likely to directly identify the type of incident except monitoring and diagnostic capabilities.

An example is a physical event that will have technical manifestations such as lost connectivity when a ditch digging machine severs the fiber link to the data center or a wiring closet burns up.

Whether the organization considers these to be security events varies, although, arguably, this will impact availability, which usually has security implications of one sort or another.

If emergency services cannot be contacted, air traffic control cannot communicate with aircraft, or credit cards cannot be authorized, it is difficult to argue that availability is not a security issue.

Validating that an incident has occurred, as in the foregoing paragraph, will generally result in the determination of the kind of incident it is.

Additional information will usually be required such as the scope and possible impact of the incident as well.

Is It a Security Incident?

There is little consensus on exactly what constitutes a “security” event, although many organizations have developed internal criteria and definitions. Organizations often consider the cause of an incident to be determinative; that is, a deliberate disruptive act would be a security matter, whereas an accident would not.

This distinction suffers from the fact that it is easy to imagine many accidental situations that can have major security implications and impacts. It may be more prudent to consider a security incident as any event that has the potential of compromising security or elevating risk, regardless of cause.

What Is the Severity Level?

Severity of an incident must be determined quickly and, hopefully, with a degree of accuracy. Declaring a full-fledged disaster as the result of a minor incident is not likely to be a good career move and neither is failing to declare one and reacting appropriately when there actually is one.

Severity levels must be defined and agreed upon, and personnel must be educated or trained to make the determination. Authority to declare the various severity levels must be assigned and escalation procedures defined.

Other preconditions exist such as information asset classification, which is required so that the criticality and/or sensitivity of affected assets can be quickly determined, which, along with the level of impact, will be largely determinative of severity level.

Once again, good diagnostics will be the key to efficiently gathering the needed information to arrive at a conclusion and initiate appropriate action.

Are there Multiple Events and/or Impacts?

Incidents can aggregate and/or cascade. That is, one threat can affect multiple resources concurrently, or an incident can initiate a chain of events, causing a “cascade” of failures, the so called domino effect.

It will be critical to determine the scope of the impact or whether there are other resources at risk as a result of an event.

Metrics and monitoring are often helpful in assessing scope but intimate knowledge of systems, networks, personnel, or facilities are likely to be needed to assess likely “knock-on” eventualities.

Will an Incident Need Triage?

Multiple events that exceed the organization’s incident response capacity to address them all will require triage to determine which issues to deal with; which to ignore, either because they are not serious or there is no ability to address them effectively; and in which order.

This capability requires substantial expertise; systems, personnel, and, possibly, facilities knowledge; a variety of real-time operational metrics about what is working and what is not; performance impacts; and so on.

For purely technical events, the typical range of data being monitored in the NOC may be adequate provided there is the expertise to interpret it correctly.

What is the Most Effective Response?

Determining the most effective response to a security incident requires the right information and knowledge of the available options.

For example, if an attacker has breached perimeter security and raised an intrusion detection alert, what action should be taken? Perhaps the network is segmented and the attack can be isolated. Perhaps the intruder can be blocked at the firewall or, possibly, more drastic action is required such as terminating the connection to the Internet.

Without adequate information and an understanding of the systems and architectures, it will be difficult to determine the least disruptive response consistent with security.

Physical compromise such as theft of proprietary information or indications of embezzlement by an insider will present even more challenging response issues. Often, the main metrics and sources of information for these types of events will be technical or accounting forensics.

What Immediate Actions Must be Taken?

Some incidents will require immediate action to avoid serious consequences. HIDS or NIDS inside the perimeter signaling an intrusion certainly qualifies. Besides validating that it is in fact an intrusion, operational metrics indicating the scope and nature of activity are critical to deciding the nature and extent of action required.

In many organizations in which operations and traffic follows consistent patterns, anomalies may be a useful metrics to warn of incipient incidents.

Which Incident Response Teams and Other Personnel Must be Mobilized?

The type and nature of an incident must be determined to make decisions about which teams or personnel will be required to deal with it.

Unit-4 (2): Security Governance and Management

Governance and Managing for More Secure Software

Governance and Security

Good governance of the security sector will generally encompass the following characteristics:

Accountability–including sanctions for breaches, and checks against impunity

Effectiveness–service responsibilities completed to a high professional standard

Efficiency–services making the best possible use of public resources in their duties

Participation–inclusive opportunities for all men and women of all backgrounds

Responsiveness –a service sensitive to the different security needs of the population

Rule of law –for all persons and institutions, including the state

Transparency–of information and processes, made available to the widest public audience where possible, or to suitable accountable institutions.

Adopting an Enterprise Software Security Framework

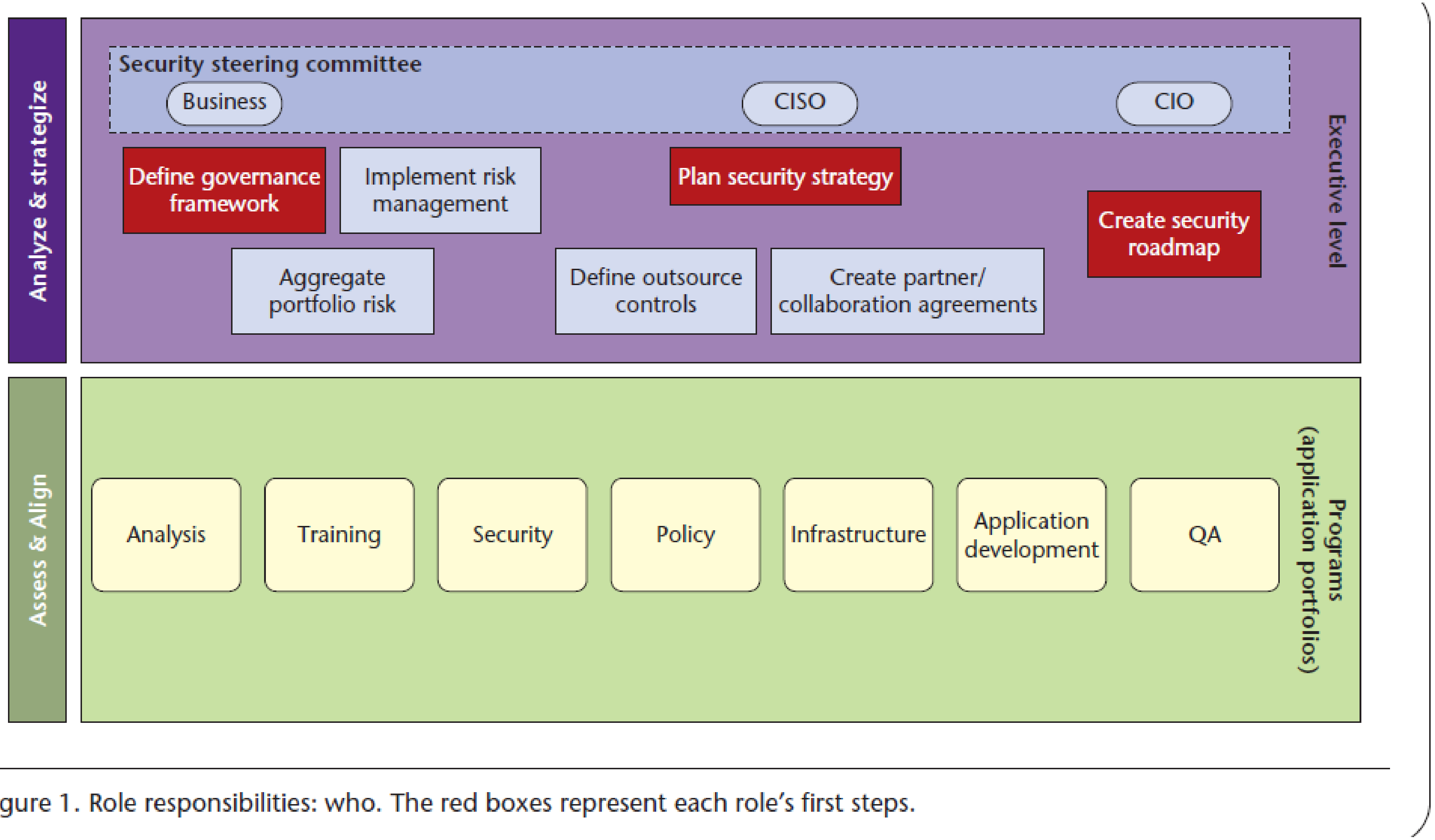

Figure 1. Role responsibilities: who. The red boxes represent each role's first steps.

Knowledge management, training.

An organized collection of security knowledge is likely to include policy, standards, design and attack patterns, threat models, code samples, and eventually a reference architecture and secure development framework.

Another element of this competency is the development and delivery of a training curriculum. Topics include security knowledge as well as help for conducting assurance activities.

This pursuit also includes new courseware, along with retrofitting of existing courseware to software security concepts.

Security touchpoints.

The definition of tasks and activities that augment existing development processes (formally or informally) help developers build security into any custom software development process, as well as in-place outsource assurance and commercial off- the-shelf validation processes. This competency defines how to assure software.

Assurance.

The execution of security touchpoint activities provides assurance—conducting a software architectural risk assessment, for example, validates that security requirements were translated into aspects of the software's design and that the design resists attack.

Assurance activities rely heavily on the knowledge and training competency to define what to look for. Tool adoption is likely to be part of this pursuit in the short-to medium term.

It will involve the purchase, customization, and rollout of static analysis tools as well as dynamic analysis aides.

Your organization might have already adopted a penetration-testing product, for instance.

Governance.

Governance is competency in measuring software-induced risk and supporting an objective decision- making process for remediation and software release.

This competency involves creating a seat at the project management table for software risk alongside budget and scheduling concerns.

Governance should also be applied to the roll out and maturation of an organization’s Framework.

The framework’s owners can measure project coverage and depth of assurance activities, reported risks (and their severity), and the progress of software security knowledge and skill creation, among other things.

How Much Security is Enough ?

- principles enacted by policies and procedures that state these requirements and risk tolerances for this asset

- clear assignment of roles and responsibilities and periodic training for staff and managers involved in protecting this asset; financial incentives for those demonstrating innovative approaches to asset protection

- periodic training for staff having access to this asset; immediate removal of access and authorization for any staff member whose responsibilities no longer require a need for access, including any change in employment status such as termination

- infrastructure architecture that fulfills these requirements, meets these risk tolerances, and implements effective controls (strong authentication, firewalls including ingress and egress filtering, enforcement of separation of duties, automated integrity checking, hot backups, etc.)

- review of all new and upgraded technologies that provide database support and in-house and remote access, to determine if any of these technologies introduce additional security risks or reduce existing risks. Review occurs before and after technology deployment.

- regular review and monitoring of relevant processes, and performance indicators and measures including financial performance and return on investment; regular review of new and emerging threats and evaluation of levels of risk

- purchasing insurance for high-impact, low-probability events

- regular audit of relevant controls and timely resolution of audit findings

Security and Project Management

Natural disasters and events such as floods, hurricanes, seismic activity, wildfires, tsunamis, volcanoes, drought, and even the ongoing effects of climate change.

Legal or statutory compliance. Depending on where in the world your project is being executed, there will be laws, regulations, forms of contract, and other statutory obligations which must be observed or followed as they relate to people, data, finances, natural resources, quality and safety standards, communication systems, security, and transparency.

Threats associated with people inclusive of theft, vandalism, malicious intent and behaviour, breaches in confidentiality, the lack of adherence to policies and procedures, terrorism, and civil conflict.

Finally, **the costs associated with security failures**. Whilst there may be no assured way to protect against every security risk, investing in and implementing suitable security policies, standards, controls, and systems can definitely reduce the costs and risk associated with its absence.

Maturity of Practice

Protecting Information

The key requirements of DSS include the following:

- Build and maintain a secure network.
- Protect cardholder data.
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain an information security policy.

Audit's Role

- Strategic alignment of information security with business strategy to support organizational objectives.
- Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
- Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.
- Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved.
- Value delivery by optimizing information security investments in support of organizational objectives.

Operational Resilience and Convergence

- reduced risk of a business interruption
- shorter recovery time when an interruption occurs
- improved ability to sustain public confidence and meet customer expectations
- increased likelihood of complying with regulatory and internal service level requirements

A Legal View

- Establish governance structure, exercise oversight, develop policies.
- Inventory digital assets (networks, applications, information).
- Establish ownership of networks, applications, and information; designate security responsibilities for each.
- Determine compliance requirements with laws, regulations, guidance, standards, and agreements (privacy, security, and cybercrime).
- Conduct threat and risk assessments and security plan reviews (for internal and contractor operations). This may include certification and accreditation.
- Conduct risk management based on digital asset categorization and level of risk.

A Software Engineering View

- the business climate
- building blocks of change, including four common pitfalls:
  - over-reliance on late-life-cycle testing
  - management without measurement
  - training without assessment
  - lack of high-level commitment (particularly relevant for governance and management)
- building an improvement program
- establishing a metrics program, including a three-step enterprise rollout:
  - assess and plan
  - build and pilot
  - propagate and improve
- continuous improvement
- what about COTS (and existing software applications)?, including an enterprise information architecture
- adopting a secure development life cycle