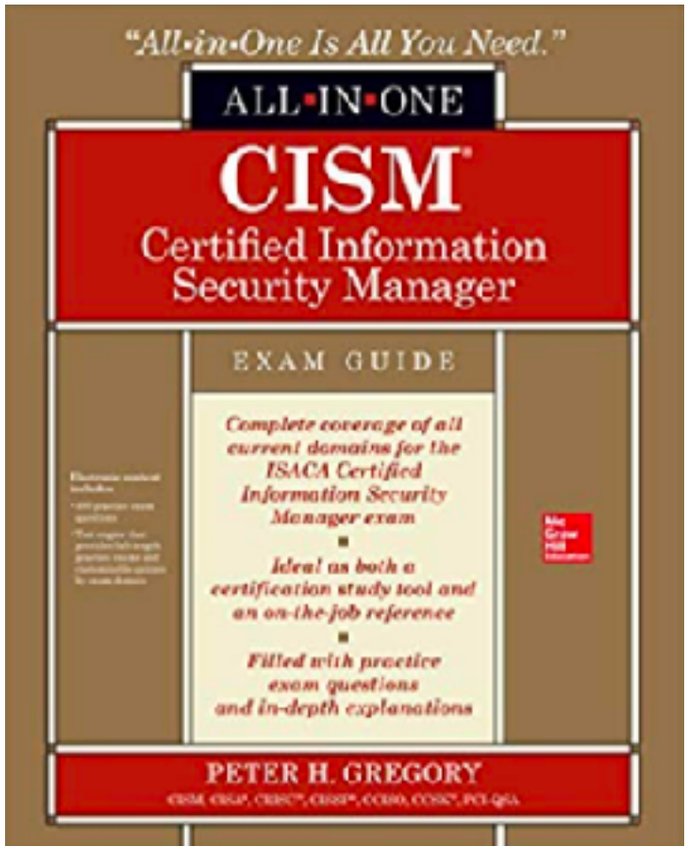
CNIT 160: Cybersecurity Responsibilities

4. Information Security Program Development Part 3

Pages 235-257



Chapter Topics

- **This lecture covers:**
  - **Policy Development (p. 235)**
  - **Third-Party Risk Management**
    - **Administrative Activities**
      - **Internal Partnerships**
    - **External Partnerships**
    - **Compliance Management**
    - **Personnel Management**

Chapter Topics For Later Lectures

- **Administrative Activities**
  - **External Partnerships**
  - **Compliance Management**
  - **Personnel Management**
  - **Project and Program Management**
  - **Budget**
  - **Business Case Development**
  - **Vendor Management**

Chapter Topics
For Later Lectures

- **Security Program Operations**
- **IT Service Management**
- **Controls**
- **Metrics and Monitoring**
- **Continuous Improvement**

Policy Development

Security Policy

- **Foundational**
- **Defines principles and required actions**
  - **to protect assets and personnel**
- **Audience is all personnel**
  - **Full-time and part-time employees**
  - **Temporary workers, contractors and consultants**

Easily Accessible

- **So no personnel can claim ignorance**
  - **As an excuse for violating policy**
- **Often personnel must acknowledge understanding of policy**
  - **At time of hire and annually thereafter**

Considerations

- **Laws, regulations, standards**
- **Risk tolerance**
- **Controls**
- **Organizational culture**

Alignment

- **Alignment with Controls**
  - **Policies and controls must not contradict each other**
- **Alignment with Audience**
  - **Policy must be understood by the workers**
  - **Avoid overly technical policies**
  - **May have a separate policy for technical workers**

Security Policy Structure

- Acceptable use of organization assets
- Mobile devices
- Protection of information and assets
- Access control and passwords
- Personally owned devices
- Security incidents
- E-mail and other communications

Security Policy Structure

- **Social media**
- **Ethics and applicable laws**
- **Workplace safety**
- **Visitors**
- **Consequences of noncompliance**
- **Cloud computing**
- **Data exchange with third parties**

Policy Distribution and Acknowledgement

- **Policy should be well-known and easily accessible**
- **High-ranking executive should inform workers that they are required to comply with the policy**
- **Executives should lead by example**

Third-Party Risk Management

Outsourcing

- **Must identify risks of cloud services**
- **You can outsource *work***
- **But you cannot outsource *responsibility***

Benefits from Use of Third Parties

- **Available skills and resources**
- **Economies of scale**
- **Objectivity**
- **Reduced costs**

Risks from Use of Third Parties

- **Higher-than-expected costs**
- **Poor quality or performance**
- **Loss of control**
- **Employee integrity and background**
- **Loss of competitive advantage**

Risks from Use of Third Parties (continued)

- **Errors and omissions**
- **Vendor failure**
- **Differing mission and goals**
- **Difficult recourse for problems**
- **Lowered employee morale**

Risks from Use of Third Parties (continued)

- **Audit and compliance**
- **Applicable laws**
- **Cross-border data transfer**
- **Time zone differences**
- **Language and cultural differences**

Identifying Third Parties

- **Inventory third party vendors in use**
- **Consult with stakeholders**
  - **Legal**
  - **Procurement**
  - **Accounts payable**
  - **Facilities**
  - **Department heads**
  - **Location-specific leaders**

IT and Third Parties

- **Ways to identify third parties in use**
  - **Established data connections with third parties**
  - **Firewall, IDS, and IPS rules**
  - **Connections to Identity and Access Management (IAM) systems**
  - **Cloud Access Security Broker (CASB) systems**

Applications to Manage Third Parties

- Allgress
- CyberGRX
- KY3P
- Lockpath
- Optiv
- Prevelant
- RSA Archer
- RSAM
- Service Now

Risk Tiering and Vendor Classification

- **Cannot perform all due diligence on all vendors**
- **Apply a level of due diligence according to the level of risk**

Criteria

- **Volume of sensitive customer data**
- **Volume of sensitive internal data**
- **Operational criticality**
- **Physical access to company buildings**
- **Access to information systems**
- **Contractual obligations**

Example

Criteria	High	Medium	Low
Customer data volume	>10M records	10K to 10M records	<10K records
Internal data volume	HR or product design	None	None
Physical access	24/7	Office hours only	None
System access	High customer data volume	None	None

Ch 4c-1

Assessing Third Parties

- **Questionnaires**
- **Questionnaire confirmation**
  - **E.g. requesting evidence**
- **Site visit**
- **External attestation**
  - **Such as compliance with SOC2, HITRUST, ISO/IEC 27001, etc.**

Assessing Third Parties (continued)

- **External business intelligence**
  - **Services like Dunn & Bradstreet or Lexis Nexus**
    - **That collect information on health of companies**
- **External cyber intelligence**
  - **Security scans**
  - **Dark web monitoring**

Assessing Third Parties (continued)

- **Security scans and penetration tests**
- **Intrusive monitoring**
  - **Third party can view internal control data in real time**
  - **Such as event logs, firewall logs, or packet captures**

Assessment Type	High Risk	Medium Risk	Low Risk
Questionnaire	Longest questionnaire	Medium size questionnaire	Shortest questionnaire
Questionnaire confirmation	High risk controls	Highest risk controls	Not performed
Site visits	Yes	Yes	No
External attestations	Required	Nice to have	Nice to have
External business intelligence	Yes	Yes	Yes
External cyber intelligence	Yes	Yes	No
Security scans	Yes	Yes	Yes
Penetration tests	Yes	No	No
Intrusive monitoring	In limited circumstances	No	No

Table 4-3 Assessment Activities at Different Risk Levels

Assessment Type	High Risk	Medium Risk	Low Risk
Questionnaire	Annually	Annually	Annually
Questionnaire confirmation	Annually	Every two years	Not performed
Site visits	Annual	Every three to five years	Not performed
External attestations	Annual	Annual	Annual
External business intelligence	Quarterly	Annual	Annual
External cyber intelligence	Monthly	Quarterly	None
Security scans	Monthly	Annually	Annually
Penetration tests	Annually	Not performed	Not performed
Intrusive monitoring	Continuous	Not performed	Not performed

Table 4-4 Assessment Frequency

Proactive Issue Remediation

- **The only means of exchange between customer organization and third party are**
  - **Money and reputation**
- **Especially when crossing national boundaries**
- **Consider enforcement mechanisms**

Contractual Provisions

- **Service Level Agreement (SLA)**
- **Quality**
- **Security policy and controls**
- **Business continuity**
- **Employee integrity**
- **Ownership of intellectual property**
- **Roles and responsibilities**

Contractual Provisions (continued)

- **Schedule**
- **Regulations and laws**
- **Warranty**
- **Dispute and resolution**
- **Payment**

Responsive Issue Remediation

- **Results from a questionnaire may be unacceptable**
  - **Such as no password change requirements**
- **Discussions with third parties may provoke changes**
  - **Or expose satisfactory compensating controls**

Onboarding

- **Process to begin a relationship with a third party**
- **Up-front due diligence**
  - **To understand the level of risk**
- **Before signing a legal agreement**

Contract Language

- **Security program**
- **Security controls**
- **Compliance**
- **Attestations**
- **Vulnerability management**
- **Penetration tests**
- **Right to audit**
- **Incident notification**
- **Cyber insurance**
- **Restrictions on outsourcing**

Security Incidents

- **Incident response is more complex**
  - **When two organizations are involved**

Administrative Activities

Internal Partnerships

Importance

- **Partnerships**
  - **Are a source of information**
  - **And help manage security**
- **Deputize team members from other groups**
- **Designate security liaisons**
- **But they need training and time allocated for these added duties**

Legal

- **Manages business risk**
  - **Through contract negotiations**
  - **With service providers, customers, and others**
- **Information security can help**
  - **With security clauses**
  - **Best if security assessment happens before signing a contract**

Human Resources (HR)

- **Recruiting: background checks**
- **Onboarding**
  - **Nondisclosure agreements**
  - **Training, including Security Awareness Training**
- **Provisioning Human Resource Information Systems (HRISs)**

Human Resources (HR) (continued)

- **Internal transfers**
  - **Move to a different department**
  - **Change access to systems and applications**
  - **Avoid *accumulation of privileges***

Human Resources (HR) (continued)

- **Offboarding**
  - **Notify security, IT and other departments**
  - **Terminate access rights promptly**
    - **To prevent revenge and sabotage**
  - **Collect company assets like laptops**
  - **Sign nondisclosure and noncompete agreements**

Human Resources (HR) (continued)

- **Training**
- **Investigations**
  - **Often in partnership with information security**
  - **Forensics and chain of custody**
- **Discipline**
  - **Demotion, time off without pay, dismissal, etc.**

Facilities

- **Access control**
- **Workplace surveillance**
- **Equipment check-in/check-out**
- **Guest processing**
- **Security guard**
- **Asset security**
- **Personnel safety**

Information Technology (IT)

- **Access control**
- **Architecture**
- **Hardening**
- **Scanning and patching**
- **Security tools**
  - **Firewalls, IDS, spam filters, etc.**

Information Technology (IT) (continued)

- **System monitoring**
- **Security monitoring**
- **Third-party connections**

Product Development

- **Security by design**
- **Secure development**
- **Security testing**
- **Code reviews**
- **Security review of open source software**
- **Developer training**
- **Protection of the development process**

Procurement

- **Due diligence for new purchases**

Finance

- **Accounts Payable is the partnership of last resort for information security**
- **Because when they get involved, the vendor relationship is already established**

Business Unit Managers

- **Security manager should understand how each department functions**
- **Develop relationships of trust**

Affiliates and Key Business Partners

- **Half of all security breaches have their nexus in third parties**

Ch 4c-2