Security Policy and Management Support

Linux Systems Security

Doing Business vs. Security

- People want ease of use, speed and flexibility when using information systems resources
- These are all good things, but are often impacted by security measures which normally make some attempt to ensure that what is happening is not exposing the organization or individual to unnecessary risks
- Integrating information systems security into the daily activities of an organization requires that resources are allocated to perform security related tasks

Resource Allocation

- Resources have costs
  - Staff
  - Equipment and software
  - Business infrastructure and process, including external
- Management support is required to obtain funding, approve activities
- Various strategies can be employed to obtain that support, the most direct being tangible cost evaluation, although intangibles can be a much larger concern to the business

Tangible Costs of Not Securing Your Assets

- Daily activity costs (paying staff) due to treating every activity as a fresh security challenge
- Business interruption costs (productivity loss) while resolving security concerns continuously and repeatedly
- Legal costs of protecting the organization from liability arising from shortcomings in security

Tangible Costs

- Direct losses in financial transactions, cyber crime
- Business development impacts due to loss of communications privacy
- Direct intellectual property loss including trade secrets, cyber espionage
- Insurance costs (e.g. liability, business interruption, etc.)

Intangible Costs of Not Securing Your Assets

- Customer trust
- Operational limitations
- Business partner trust
- Investor perceptions
- Organization liability for partner and client information
- Marketability of a secured business

Define Security Policy

- A systems security policy is a way of codifying the various activities and guidelines associated with security in order to enhance understanding, consistency, implementation, and responses
- The policy is written to identify threats and describe strategies to mitigate or eliminate those threats while minimizing exposure to them
  - Tie into the organization's overall risk management strategy
  - Incorporate legal obligations of the business with regard to privacy laws and consumer protection laws where applicable

Security Policy

- Like all policies, systems security policies should be regularly reviewed for applicability, effectiveness, and enhancement - outdated policies can do more harm than good
- Modern organizations make heavy use of short-term, part-time, and contract workers - your policies and system architectures must support the necessary compartmentalization of services and data to limit exposure when these types of workers require information systems resources
- Sample policy documents can be obtained from the SANS Institute and other online sources
- Include at least those elements of your systems security that address the main recognized threats to your business

Main Recognized Threats

- From ‘Study of the Impact of Cyber Crime on Businesses in Canada.’ International Cyber Security Protection Alliance (May 2013):
  - Malware and virus attacks
  - Sabotage of data or networks
  - Financial fraud
  - Phishing/social engineering
  - Theft of devices, particularly mobile devices
  - Unauthorized access or misuse of websites
  - Denial of service
  - Telecommunications fraud
- From ‘Project 2020’ International Cyber Security Protection Alliance (October 2016):
  - Intrusion for monetary or other benefit
  - Interception for espionage
  - Manipulation of information or networks
  - Data destruction
  - Misuse of processing power
  - Counterfeit items
  - Evasion tools and techniques

For more up to date and complete reviews of current cyber crime threats:

Canadian Centre For Cyber Security

Services Security

- Needs assessments define user access requirements
- Implement data encryption when data is considered private to the organization but is exposed to people or systems not under the organization's control, methods of identifying the sensitivity of information need to be part of this
- Firewall and proxy services, both inbound and outbound

IT Services Security

- Deployment and configuration have security components
- Security status verification plan and reporting
- For any of these to be successful at interdicting attacks, the implementation must faithfully enact the policies, ongoing policy management and campaigning to make security second nature in the organization are required

Security Policy Management

- Social engineering relies on ignorance, uncertainty, and perceived personal benefit without regard for consequences to others - management must be prepared to invest in training and institute consequences for non-compliance (e.g. retraining, oversight, performance improvement plans, etc.)
- Include general guidelines to avoid the "deal with the devil" syndrome which corporate lawyers sometimes use as justification for blocking policy creation and implementation
- Security policies need visible management support and compliance

Security Policy Management

- Consider creating multiple levels of policy documents at different levels of abstraction to reduce work required to adapt to business change
  - Exec level - User authentication will be implemented for all user access
  - Management level - Login services will use 2 factor authentication, web services use ...
  - Staff level - Employees will be required to have passwords of enforced complexity, changed on an enforced schedule, use VPNs for remote access, etc.
- Incorporate feedback mechanisms so that people affected by the policies can provide valuable input on how those policies might impact them

Security Campaign

- Security policy awareness requires regular reinforcement and update, ensure new employees get exposed to the policies rapidly and consider insertion of systems security-specific clauses in new-hire agreements and contracts with third parties
- User compliance is required for plan success, the policies should be written with regard for corporate culture and make clear statements regarding benefits of compliance and the roles and responsibilities of the users and other parties
- Policy components need to have justifications that can be understood by the people they affect, use loss experience examples whenever possible to help "make it real"

Security Awareness

- Use multimedia (websites, audio, video, posters) to reach a wider audience, emails don't suffice - do "security marketing" including obvious guidelines as well as company-specific policies (e.g. https://www.youtube.com/watch?v=UPs5JCg910E)
- Consider creating events around security or include a security session in corporate development activities

Resources

- Office of the Privacy Commissioner
- Canada's Cyber Security Strategy
- SANS Institute Security Policy Whitepaper
- SANS Sample Policy Documents
- FCC Cyber Security Planning Guides
- Microsoft Security Planning Guide
- NIST Security Awareness and Training Program
- NIST Publications