

Getting Executive Buy-in

Tips & Strategies



Agenda

- Why Security Is Important To The Business
- Why Management Buy-in Is Needed
- Strategies For Obtaining Management Buy In
- Case Studies

Why Security is Important

- Reputation
 - Reputation is about protecting the BRAND/public perception
 - What is your organizations reputation worth
 - What will happen if there is a negative security event
- Business Asset Protection
 - Intellectual Property
 - Customer Data
 - Employee Data
- Legal
 - There are various compliance laws that will apply in just about every organization
 - Some sectors have more strict laws on privacy and security (Healthcare, Finance, other)
 - Legal requirements as a business driver for security is good way to start

Why Management Buy-in is Needed

- Security transcends:
 - Departmental Silos
 - Physical, logical, and electronic boundaries
 - IT Disciplines: systems, network, applications
- Affects Operations
 - Information is a valuable corporate asset
 - Protection of information is a management responsibility
 - Corporate Governance/Risk Management
 - Security Failures are “management” failures that have organization wide impact on operations

Obtaining Management Buy-In

1. Communication is key

- Speak the language
 - Monetary and business risk vs. technical jargon
- Fear Uncertainty and Doubt (FUD) does not work
 - Fear is not a justifiable business case
- Keep your message short
 - Executives can be very busy, keep message succinct
- Follow up regularly
- Metrics, charts and figures
 - Pictures sell
- Soft skills
 - People skills are more important than the hardware and software

Obtaining Management Buy-In

2. Focus on the big picture

- Tie efforts to corporate goals
 - Core values
 - Corporate mantra
- Speak to operational abilities
 - By implementing x, we can do y and z
- Security as a business enabler
 - Show how efforts enhance user experience
 - E.g. Single Sign On
 - Find out the needs of the business and help make that easier
 - Show ROI if possible
- Be practical
 - Balance protection with value of data
 - Don't spend \$100 to protect \$10
 - Make decisions that raise the level of security as the risk is raised

Obtaining Management Buy-In

3. Find your security champion(s)

- Power in numbers
- Demonstrate how management can lead by example
- Local office POC/responsible party
 - Similar to company fire marshal

4. On-going learning and adaptation

- Stick vs Carrot Approach
 - Stick- fines, reputation, prosecution
 - Carrot – reduce costs, reduce risk, improve manageability, improve public perception
- Don't be in a hurry
 - Seed the idea today and let it grow
 - Culture change
- Case studies
 - A wise man learns from the mistakes of others

Laws

- Regulatory Requirements
 - Electronic Communications Privacy Act
 - Gramm-Leach-Bliley Act (GLBA)
 - Health Insurance Portability and Accountability Act (HIPPA)
 - Family Educational Rights and Privacy Act (FERPA)
 - Sarbanes-Oxley (SOX)
- Cyber Crime
 - USA Patriot Act
 - Computer Fraud and Abuse Act
 - States Security Breach Notification Act
 - Economic Espionage Act
 - Digital Millennium Copyright Act

Case Study: CVS Pharmacy

- Represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access
- July 2006 and continuing into 2007, television stations and other media outlets reported finding personal information in unsecured dumpsters used by CVS pharmacies in at least 15 cities throughout the United States. The personal information found in the dumpsters included information about both CVS's customers and its employees

Case Study: CVS Pharmacy

- For failing “to employ reasonable and appropriate measures to prevent unauthorized access to personal information”
- CVS agreed to:
 - Pay \$2.2 million
 - Establish, implement, and maintain “a comprehensive information security program”
 - Designate a person to “be accountable for the information security program”
 - Identify “material internal and external risks to the security, confidentiality, and integrity of personal information”
 - design and implement “reasonable safeguards to control the risks”
 - Require “service providers by contract to implement and maintain appropriate safeguards”
 - Obtain an independent 3rd party assessment every 2 years for “twenty years after service of the order”

Case Study: Major City's Municipal Courts

- On Wednesday, February 4th the “Virut” virus was discovered
- The virus infected 475 out of 16,000 computers (> 1%)
- The court system was shut down over the weekend and during the entire week of February 9th
- Hearings and Jurors during that time had to be re-scheduled
- The city tried to get the word out about the closure on Friday and over the weekend, but some didn't hear the news in time...there were hundreds of frustrated citizens

Case Study: Major City's Municipal Courts

- Affected city's 311 help line
- Workers were still receiving phone calls and they had to write down the details manually
- Impossible to track work orders
- It took the city more than a week to recover systems and return operations to normal (2/4 – 2/13)
- A contractor (\$25,000) was also used to help restore systems