Building a Security Program

Presented by

Tim Brown  CISSP, CISA
Executive Director
IT Leaders

What I Think I Do

What My Mom Thinks I Do

What Finance Thinks I Do

What Business Users Think I Do

What Business Users Want Me To Do

What I’m Actually Doing
Security Program vs Plan?

- What’s the difference?
- Program – a larger view showing your overall security efforts
- Plan is a part of your program
Security Program

- Charter - showing mandate and scope
- Vision statement – security principles, components, and framework
- Governance – steering committees, accountability, reporting framework
- Plan - strategic view of goals and objectives
Security Program

- Should be short and concise
- Should be **REALISTIC**
- Should be a living document
- Should meet the overall needs of the organization, not just to the IT unit
Security Program - Charter

- May sound overly formal, but is important
- Spells out the mandate for the security organization and its authority to act
- Important even for a security organization of one
Security Program - Vision

- Again may sound overly formal, but is important
- Lay out core principles
  - Should stress the importance of business needs
  - This will help you get buy in from constituents
Security Program - Governance

- Ensures high-level business requirements are defined and met.
- Who does security report to?
- Accountability – steering or advisory committee.
- Policies – may not list the actual policies, but gives a framework for how policies are developed, approved, and where they are published.
Security Program- Plan

- Important to first describe current state of security
- Describe your target state
- The gap between the two will help lay out your strategic direction
- Should be updated annually, even though some projects may take many years
Security Program- Plan

❖ Goals:
❖ Should have short, medium, and long term goals
❖ Should be measurable
❖ Risk management process will help feed security plan
❖ Security requires layers, so your strategic plan should, as well
Security Program - Plan

❖ Goals:
❖ Should be strategic, but show specific projects
❖ Lay out detailed plan for each
❖ Include budget and resources needed for success
❖ Include deliverables
Security Program- Plan

- **Goals:**
  - Should be realistic
  - Don’t just buy stuff
  - Should include timelines, realizing that some goals may take more than one year
  - Should link to the organization's business needs and strategic direction
Security Program- What’s next?

- OK, you have written out your program and your plan
- You need buy-in from:
  - Management to fund it
  - IT Team to implement it
  - Constituents/Users to follow it
- You cannot MAKE them follow it, you have to convince them
Security Program- Selling it

- Upper management-Why should they?
- You need authority and funding
- It is difficult to show a savings for implementing security as it is more about cost avoidance
- You need to show why it is important to them:
  - Reduce risk
  - Protect staff and students
Security Program - Selling it

- IT Team - Why should they?
- You need their cooperation and skills
- Get their input on the technology
- Show how it can make their jobs easier
Security Program- Selling it

- Constituents/users-Why should they?
- They have to follow the new polices and procedures
- Show them WHY they need to participate in the program
- Getting their input shows they are part of the program, not victims of it
- Again, show how it can make their jobs easier
Located in Tallahassee, Florida, NWRDC was founded in 1972 as one of four regional data centers serving State University System of Florida. We have been providing services for over 44 years.
NWRDC: Who we are...

- Operates as a 100% self funded not-for-profit auxiliary of Florida State University; no external state funding

- Provide services to universities, colleges, K12, as well as city, county, and state government entities

- NWRDC designed and engineered to be a state-of-the-art data center that can guarantee customers’ security, accessibility and connectivity
NWRDC: Who we are...

- Shared governance
  - Organizationally report to Assoc. VP & CIO of FSU, Michael Barrett
  - Operationally report to a Board comprised of our customers (Chair, Mehran Basiratmand, CTO of FAU)
  - Shared Governance is the **KEY** to success.
Customer Distribution
NWRDC Services

- Collocation and Disaster Recovery site (hot, warm, or cold)
- Managed services
- NWRDC Community Cloud
  - Cloud Infrastructure as a Service
  - Storage
  - Backup as a Service
  - Public Cloud Services via commercial partners
NWRDC Services

- Mainframe Hosting
- Tallahassee Fiber Loop
  - Connectivity to the FLR (10Gb)
- Security Services
  - Partnership with SecureWorks
Thank You

Questions?
Tim_Brown@nwrdrd.fsu.edu
www.nwrdrd.fsu.edu