Security Expansion Through Risk Analysis

Leveraging Corporate Risk to drive Security Expansion

Rob McComber
Cyber Security Manager
Smart Infrastructure Innovations, Schneider Electric
robert.mccomber@telvent.com

Schneider Electric

THINK BIG

Critical Infrastructure Security Goal:

To ensure the security of our critical infrastructure assets through the use of **any** technical and operational tools available

Today's Landscape

- Security is no longer special
- Critical Infrastructure security is just one part of the corporate security challenge
- Businesses expect security goals to be achieved
- Effective security relies on leveraging other groups to reduce risk

'Security is a process, not a product' – but not necessarily in the way you think
…so what defines a process?

Security - A Growth Area

- Threats and vulnerabilities are a growth industry – security as a field must keep up
- Security professionals often focus on specific threats at a tactical level – opportunities for mitigation of a class of threats can be missed
- Mitigations and responses are predominantly technical in nature
- Business-level mitigation is far less common as are business cases for holistic approaches to security

Security often acts as an umbrella for tasks which cross many verticals within a company, increasing the appearance of high cost

Self-Induced Constraints

- The longer we continue to treat OT security as wholly different from other aspects of corporate activity, the greater the rift becomes
- OT security teams typically focus on what makes them unique
- Corporate security teams are often perceived as adversaries
- Often very limited awareness of corporate initiatives in other departments (Legal, Education, IT)

Results of Excessive Constraints

By looking only within our own scope for solutions we:

- Fail to recognize threats rooted beyond our boundaries
- Fail to leverage solutions which can only be implemented by others
- Risk inefficient solutions that fail to take advantage of corporate assets
- Limit the visibility of our activities

Driving Investment

What directly justifies expanding a security program, or applying additional funding to current security projects?

- New classes of threats to the operational systems or networks
- New legal or regulatory requirements
- Existing threats or vulnerabilities which may not have been mitigated fully become more significant

…but what can you do to continue improvement when you're not able to demonstrate these types of changes?

Demonstrating Value

When delivering a business case for security-related initiatives, it is important to demonstrate ALL value, direct and indirect;

Direct Value Core Value

- Which specific operational threat(s) to critical infrastructure is mitigated by this action? (your target)

Direct Value Additional Benefits

- Which other vulnerabilities / risks are mitigated by this action? (not necessarily within your scope)

Indirect Value ‘Ripple Effect’

- What tangible products are created which benefit the company overall? (are re-usable products created?)

Understanding Risk

- Risk is the result of analyzing threats to an asset or process, the likelihood of those threats being realized, and the potential impact of that realization
- Quantifying risk allows asset owners to prioritize activities aimed at reducing their exposure to threats
- Aggregating risk across different levels in an organization provides a mechanism for leadership to recognize ‘clusters’ of issues which can be more effectively addressed through common solutions

Risk portfolios are commonly used to evaluate risk across a large enterprise or division

Using a Risk Portfolio

Security risks are often reviewed in isolation both from each other and from operational risks

- Risk portfolios support evaluation of ‘global risk’ across multiple verticals
- Particularly useful when security is spread across multiple reporting chains
- Mitigations can be applied at higher levels within the company, affecting broader levels of exposure
- Natural Hedges’ can be identified more easily through the use of a Risk Portfolio

A ‘natural hedge’ exists when one activity within a company offsets risk associated with another

What does this all mean?

- By assessing risk at a higher level, requests for additional security investment can take new forms:
  - Determination that the risk is sufficiently mitigated at a higher level
    - Example: a low-impact risk may be covered by corporate insurance
  - Recognition that mitigation of the risk is more appropriately performed by another group in the company
    - Example: Requirements for background checks for OT personnel are already performed by Human Resources annually
  - Determination that another group within the company should be mitigating the risk under their budget
    - Example: Security training for OT field personnel should be developed and prepared by the Corporate Training group
  - An issue identified at the OT level is actually a systemic corporate issue and must be mitigated across the entire company
    - Example: Unauthorized use of personal cellular devices on workstations or wireless networks

Leveraging Attack Trees

Attack trees provide an organizational mechanism to determine root threats within a complex system.

- Trees assist in identifying key points where a specific action can mitigate a broad range of threats- ‘choke points’
- Attack trees assist professionals to recognize potential vulnerabilities which may not be readily apparent through other forms of modeling

- When combined with a Risk Portfolio, Attack Trees can be very effective at determining the most appropriate group within a company to mitigate a threat
- …and to fully demonstrate the groups which benefit from the mitigation

A Risk-based Process

Identify risks and perform root cause analysis

Align risk analysis results with corporate risk portfolio

For each CI risk, determine if a higher-level corporate risk or mitigation exists

Develop a business case focused not only on the CI benefits but also on the broader corporate benefits of a specific mitigation

Collaborate with other groups to identify the best-positioned department or vertical to implement the mitigation

Questions to Ask

When establishing a security program against future requirements, consider;

- Maximize utilization of existing assets
  - Can I use the tools I have today? Or use them more effectively?
- Leverage other programs / technologies in the company
  - Can I reduce risk to a tolerable level with support from other groups?
- How do my product lifecycles align with my security needs?
  - Can I meet new requirements in a short timeframe with an upgrade?
  - Will investing now undermine a planned product investment?
- Is there a natural hedge for any of the current risks?
- How much risk do I face in addressing these issues now?

Supporting Groups

- Corporate Risk Management / Governance
- Corporate Quality and Compliance
- Corporate IT
- Corporate Legal Teams
- Corporate Education
- Facilities / Operations Groups