Welcome to SecTor

SOC, Managed Services and Risk

Matt Anthony
VP Security Remediation Services
manthony@herjavecgroup.com
@mattanth
A Discussion

An enterprise viewpoint.
How I think about information security.
I think we spend too much time thinking about security controls, and not enough time about what they’re doing.

And a bit of advice about Incident Response
It’s all about Risk

- Risk Management, actually…
- What are you doing to measure, understand, report and treat Information Security Risk?
- Is Information Security Risk defining and supporting your security program?
- Are we too focused on external events?
- Do we fully understand the risk profile and risk tolerance of our enterprise?
- Does the enterprise understand the risks we present and report?
It’s all about RISK

• Treating risk by:
  • Avoiding it – Just stop doing the risky things (or get your business to stop). This leads IT Security to being the “NO” people, and that just doesn’t work very well.
It’s all about RISK

• Transferring it – Insurance helps, and so does getting someone to share your responsibility.

• Mitigating it – Doing the risky things in less risky way.
  – Security controls – technologies, processes, governance

• Accepting it – A lot of risk is accepted by the wrong people or at the wrong level, or without clear reporting.
  – This is the most important message in a risk discussion. It’s probably not your job to accept risk.
Security Operations Centres

• Do you have a SOC?
• Does your SOC manage risk – and how?
What is the modern SOC doing?

- 24/7, 365 is just expected
- Global threat intelligence
- Multiple technologies
- Global reach
- Highly skilled analysis
- Secure physical location
- Vigilant background checks on resources
What are the Risks of DIY SOC

• Not enough training of analysts
  • They’re hard to get, and hard to keep
• Corporate commitment to space, tools
• Resource conflict with other operational requirements
• Size
  • Will you see enough events to recognize threats early?
  • Will your staff see enough events to stay sharp and focused?
  • In peak times, will you have enough resources to cover major issues?
• What you see, what you don’t see, what you think you saw…
Managed Services

• Managed SOC, your issues
  • Risk transference
    • Your partner takes on the capital and human risks for delivery
  • Risk avoidance
    • You can stop doing the risky business of SOC
  • Risk mitigation
    • You have to make a decision – can I do this better – manage the risks of events, alerts and SOC management – lower the risk profile of my organization – better than a specialist?
    • Size matters.
  • … but not acceptance. You always stay in control.
Incident Response and Remediation

• Are you prepared?
• My advice is simple:
  • Have a documented and tested plan.
  • Communicate with the business leaders about risk.
  • Have a partner you trust for surge capacity.
  • Don’t wait until you’re breached.
• NIST 800-61r2