Build your security culture on the risk management expense

Ana-Maria Matejic

Principal consultant/co-founder

Who are we ?

- A team focused on providing consulting services
- Our background is our “silver bullet”
- Distributed team but with a single vision

What do businesses want ? Resilience…

- Hot topic in business not only in “cyber” world
- Resilience = something you realize you have *AFTER* an event has happened
- Simply put :
- *level of resilience determines who succeeds and who will fail*
- HBR defines resilience as

The skill and the capacity to be robust under conditions of enormous stress and change

From resilience to “cyber-resilience”

- Relatively new term
- Describes flexibility and responsiveness in front of a cyber-attack
- It’s a “proactive” rather than “reactive” defense approach
- “Bend” or “break”
- 4 elements
  - Manage & Protect – Technologies / Policies / Trainings
  - Identify & Detect – Active detection
  - Respond & Recover – Incident Management / Business Continuity
  - Govern & Assure – RM program / Board-level commitment

People ask…

- *How is cyber-resilience different from cyber-security ?*
  - Both aim at keeping business operational
  - Cyber-security : focuses to keep out an attacker and protect the data
  - Cyber-resilience :
    - Designed for the “always-on” era
    - focuses on continuity of operations in the event of a disruption (breach)
    - Assumes understanding the 3 phases of an attack : Before – During – After
    - Preparation for each phase makes a difference in the cost of a breach

The 4 elements and risk

- Cyber-resilience's principles look at enterprise-wide **risk** factors to:
  - Simplify design and implementation
  - Continuous review of critical assets, attack surfaces
  - Know the critical processes
  - Focus on ***both*** technology and human aspects of end-to-end BC
  - Implement enterprise-level risk management and governance

The “before”

- Can last as long as the attacker wants – scouting time
- What can the company do ?
  - Start building the culture **not only** the awareness
  - The 7 pillars of security culture

  attitude - behavior – cognition – communication – compliance – norms - responsibilities
  - Management – IT staff – non-IT staff
- Design the systems with the “end” in mind
- Think beyond the firewalls , IDS/IPS and other technologies
- It’s the right time to think about “during” and “after”
  - “cybersecurity 101” = basics

The classical talk is about awareness

- Awareness of what ? YES, we are aware ☺
- In most of the organizations we hear
  "we run regular awareness trainings" / "our employees score maximum"
- But then we come in and perform risk assessments with a wide scope
  "I was on holiday, *left the customer db password* with my team-mate"
  "I *hate* to wear the badge so I used my friends' when we went out of building"
  "*Occasionally* we run security controls review"
- The security industry views the average employee as the "weakest link in the chain" to justify investments

Let’s look at the effect

- If we look around : the most recent cyberattacks used the human vulnerability
- Can we fix this 100% ? No guarantees
- Organizations get in “buying mode” as a compensatory control
- But is it really about buying one more product?
- What does it mean for the organization ?
  - Halt of operations
  - Can extend to a national threat ? (look into the Ukrainian power-grid attack)

…but address the “cause”

- Sometimes business processes and security controls don’t align
- We can have great security ecosystem but a management approach “nobody understands what they do there”
- Results of risk assessments are sometimes not very bright and feel like pointing the “guilty one”
- A critical function not accepting risks = the organization doesn’t have a risk culture
- T-CSO vs B-CSO – can make a big difference
- Understanding how the 3 pillars : people – tools – processes interact is little understood

Start from the basics

*The **ideas**, **customs** and **social behavior** of a particular people or society that allow them to be free from danger or threats. –*

The Security Culture Framework

THANK YOU! QUESTIONS?

advise@xelerate.eu