TREXIN INSIGHT PAPER

November 2016

SECURITY AND ORGANIZATIONAL MATURITY

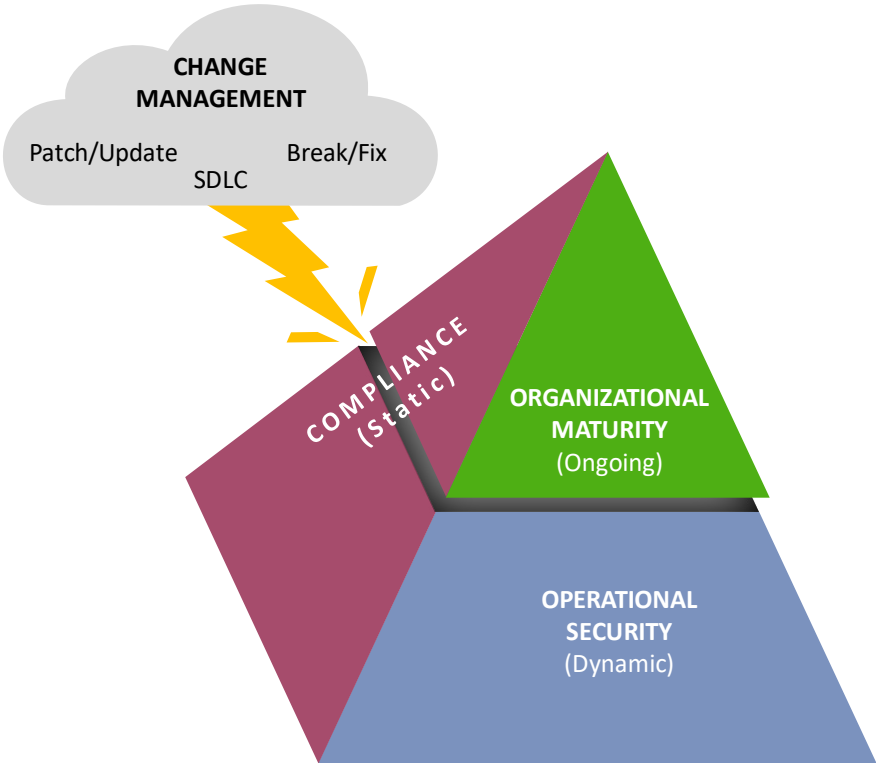
It's Not Just about Firewalls and Checklists.

Although I am the Chief Security Officer at Trexin, for a long time I resisted working directly in the Information Security field. Back at Bell Labs, we did not talk specifically about security—UNIX and the Internet were developed as trust-based systems. But we did believe passionately in privacy, and that culture shaped my thinking. I remained in the operations and application delivery corners of IT for the longest time, and found that my cybersecurity background suited me to face off with auditors while still representing the interests of IT. I found that compliance could be a force for good (yes I really typed that!), and delivered a number of "impossible" projects using the lever (sledge hammer?) that "it's needed for compliance". This also shaped my thinking.

I'm not the only cybersecurity professional with an eclectic background, and several of us who know what "eclectic" means have been talking about a broader framework for cybersecurity, more suited to the Board Room role we aspire to have.

Here at Trexin we draw the overall cybersecurity picture as follows:

Change Management: the lightning bolt that destabilizes Operational Security; mitigated by the Organizational Maturity of the enterprise.



Let's look at the various layers.

OPERATIONAL SECURITY

By "Operational Security" we mean most if not all of what you are thinking when you think of cybersecurity: firewalls, anti-malware, intrusion detection, honeypots, data leak prevention, encryption, data classifications, Incident Control Centers, etc. There are vendors to provide equipment, vendors to manage as a service, vendors to poke and penetrate, metrics and dashboards, all of the stuff that makes up an information security

infrastructure. It is a dynamic environment, that needs to be able to detect, triage, react, and then later forensically investigate down to the minute if not second.

COMPLIANCE

There are a number of fine security/privacy compliance frameworks, and good Wikipedia articles on each:

- CoBIT (https://en.wikipedia.org/wiki/COBIT)
- PCI DSS (https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard)
- NIST 800-53 (https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53)
- HITRUST (https://en.wikipedia.org/wiki/HITRUST)
- 20 CSC (https://en.wikipedia.org/wiki/The_Center_for_Internet_Security_Critical_Security_Controls_for_Effective_Cyber_Defense)
- etc.

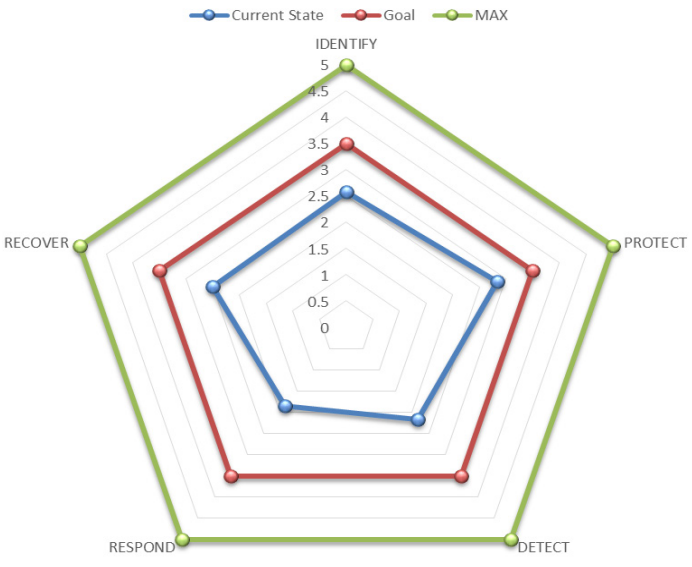
Trexin describes it as static rather than dynamic, since any attestation is necessarily a point-in-time **at the time of assessment**. The truth is a bit more complex, since they also check for ongoing governance and controls, and require periodic checks and reassessments, but overall static compared to Operational Security.

ORGANIZATIONAL MATURITY

"Organizational Maturity" is a key insight and the driver for writing this piece. When launching **Trexin's Cybersecurity Risk Assessment** offering (http://www.trexin.com/cybersecurity/), we decided to combine the NIST CIC framework with SEI's Capability Maturity Model (https://en.wikipedia.org/wiki/Capability_Maturity_Model). Our thinking was that true cybersecurity resilience is more than just IT, and more than just a checked box on a compliance checklist. Enterprises should get credit for having smart people making heroic efforts to manage and mitigate risks, but also understand that

Figure 1

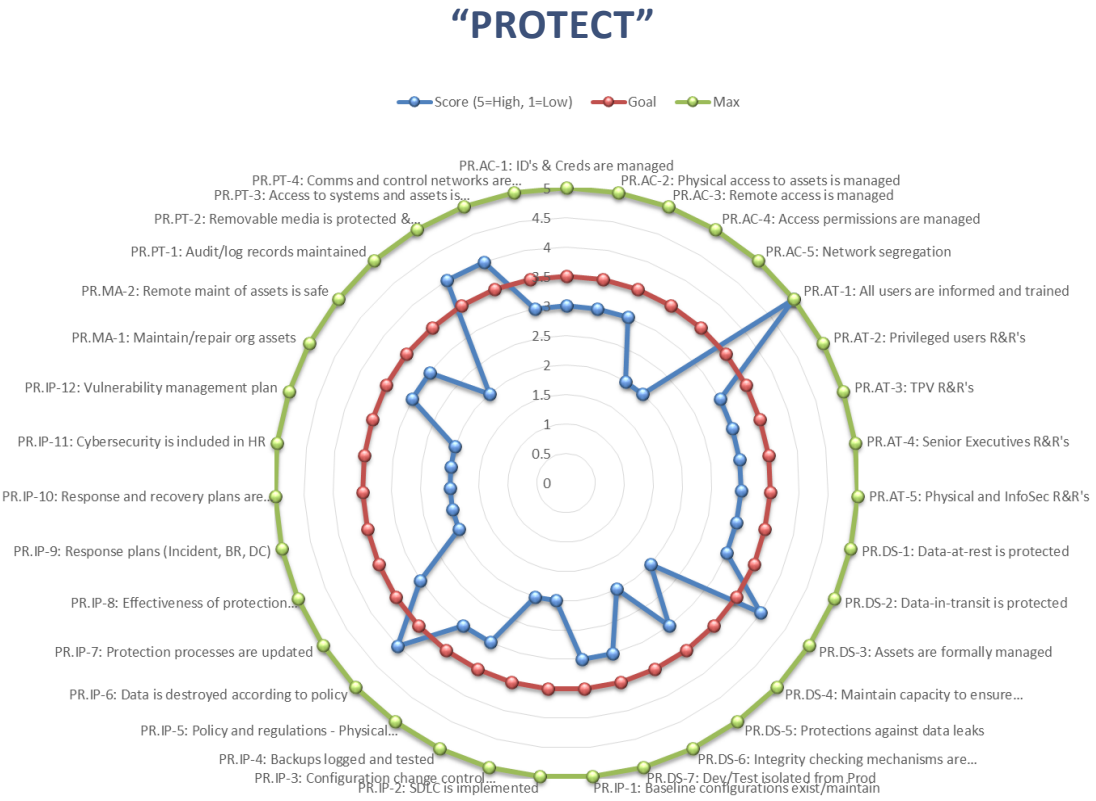
CURRENT STATE RISK ASSESSMENT



Function	Current State	Goal	MAX
IDENTIFY	2.58	3.5	5
PROTECT	2.83	3.5	5
DETECT	2.17	3.5	5
RESPOND	1.86	3.5	5
RECOVER	2.50	3.5	5

such protection is a fragile shell. So we assigned a "maturity score" using the CMM 1-5 scale, and would come up with high-level assessments like Figure 1 above.

That also drills down into each CIC Function like this:



ISACA's, the professional IT governance organization, acquisition of the CMMI in 2016 (http://www.isaca.org/about-isaca/pages/cmmi.aspx) is evidence that our model is the wave of the future.

CHANGE MANAGEMENT

When I was part of the Mergers & Acquisition teams at banks and healthcare insurers, I was able to shorten my due diligence time dramatically, often to 2-3 days. My trick was to focus on the Systems Development Life Cycle at the target company, and very specifically on the protection of data as it moved from development, to test, to production. I invariably found this to be the weakest security in the company, and it makes sense: Operational Security's mission is to ensure operational stability, and any change to that environment is potentially a threat. Planned changes, no matter how well controlled by Change Management, require purposeful acceptance of operational instability. This weakening of controls (for example, normal-traffic monitors for web sites) need to be turned off during load testing, and "normal traffic" signatures need to rebuild after deploying significant web site changes.

So in the graphic on Page 1, we represent Change Management as a lightning bolt that destabilizes Operational Security, mitigated by the Organizational Maturity of the enterprise.

LESSONS LEARNED

Cybersecurity is increasing in complexity as technology evolves and threats evolve—but the old threats and vulnerabilities remain. On the plus side, we have faced (and mastered) situations of increasing complexity elsewhere (computer chips and systems, air traffic control, the World Wide Web, etc.). The insights presented here are recognizably part of the solution in these other fields. Points to keep in mind:

- Don't treat this as strictly a technical problem
- Cherish Operations as the top priority and consider even "improvements" as risks to be mitigated
- Never forget the importance of government compliance
- Keep in mind the human and organizational aspects of the system
- When in doubt, always "follow the data", to stay focused on the key risks and weaknesses in your systems and processes

Trexin has extensive experience "in the trenches" of aligning organizations while delivering. Contact us to learn more, get more pragmatic advice on how to "get it done", or to have challenging conversations that could lead to interesting and beneficial results.

This TIP was written by Glenn Kapetansky, a senior principal, who specializes in financial services and healthcare & life sciences. Glenn welcomes comments and discussion on this topic and can be reached at glenn.kapetansky@trexin.com.