Moving From Security to Governance, Risk, and Compliance? Campus Perspectives Panel

Joe St Sauver, Ph.D. (joe@uoregon.edu)

Internet2 Global Summit, Denver Colorado

Tuesday, April 8th, 2014 8:45-10:00AM

Governor's Square 11

http://pages.uoregon.edu/joe/security-to-grc/

Disclaimer: all opinions expressed are strictly my own.

A Lot Has Been Changing in Security, Particularly in the Higher Ed Community

- **Higher ed organizations** that have been involved with security have been evolving (including the Higher Education Information Security Council (HEISC).
- **Personnel and their roles** have also been changing, and some higher ed security activities have (for whatever reason) seemingly have gone dormant.
- **Security threats haven't disappeared**, however. We're still seeing as many or MORE technical security threats as in the past.
- **Our topic today, however, relates to the (potential) evolution of higher "operational/technical security" to "governance, risk and compliance" (hereafter "GRC").**

Paul Proctor (Gartner) on "What Is GRC?"

- "GRC is the most worthless term in the vendor lexicon. Vendors use it to describe whatever they are selling and Gartner clients use it to describe whatever problem they have. For seven years I have battled this monolithic term and I fear I'm losing the battle. The alternative is to try to bring some clarity to its usage by defining some boundaries.

- "Here is our published GRC definition, which I [e.g., Paul Proctor] like[s]:

  "GRC is neither a project nor a technology, but a corporate objective for improving governance through more-effective compliance and a better understanding of the impact of risk on business performance. Governance, risk management and compliance have many valid definitions. The following definitions illustrate the relationship of the three terms and serve for Gartner's GRC research:

  - Governance — The process by which policy is set and decision making is executed.
  - Risk Management — The process for preventing an unacceptable level of uncertainty in business objectives with a balance of avoidance through reconsideration of objectives, mitigation through the application of controls, transfer through insurance and acceptance through governance mechanisms. It is also the process to ensure that important business processes and behaviors remain within the tolerances associated with policies and decisions set through the governance process.
  - Compliance — The process of adherence to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements."

- http://blogs.gartner.com/paul-proctor/2013/05/13/why-i-hate-the-term-grc/

Operational/Tech Security vs GRC

- **Operational/Tech Security:**
  - **Technical focus**
  - **Audiences:** users, "techies"
  - **Practitioner background:** often computer science
  - **Tools:** improved coding, encryption, active scanning, passive monitoring, firewalls, anti-virus, forensics, etc.
  - **Success?** system usable and not hacked/cracked; no breach of PII, etc.
  - **Some Challenges:** personnel (huge demand for technical talent, limited pipeline); resources (huge population to help but few resources); security v. user convenience
- **GRC**
  - **NON-technical focus**
  - **Audience:** board, sr. execs, auditors, policy folks
  - **Practitioner background:** often law, public policy, management, etc.
  - **Tools:** statutes/regulations/ policies, plans, audits/other reports, cost analyses, resource allocation choices
  - **Success?** Followed plan and on budget; complied with all laws/specs; no bad publicity.
  - **Some Challenges:** still seeing breaches even when "fully compliant;" all that "techie" security stuff...

CIOs/CISOs And How We're Getting To GRC...

- Assume you're a Chief Information Officer (CIO) [or maybe a Chief Information Security Officer (CISO)].
- Cyber security is increasingly "in the news."
- Executive leadership wants to know "what's going on" in cyber security and "what steps are being taken to keep our institution safe?"
- Given the "importance of the issue" you've been given a "long" presentation slot (e.g., ten minutes) at the next executive leadership meeting to explain "in detail" what's being done [including five minutes for Q&A].
- Members of the executive leadership team are smart men and women, but they're juggling a million other major issues, too, and they're not really highly technical people.
- ***So what do you cover during that session?***

Maybe Operational Security Issues?

- The implications of MS Windows XP going end-of-life and no longer getting security patches from Microsoft, including your strategy for handling those EOL systems?
- Recent attempts to phish members of the campus community, and the role of multifactor authentication?
- Cryptolocker and other major recent malware threats?
- New results from scanning the campus for hitherto-unknown caches of personally identifiable information?
- The security benefits of the latest cloud-based security application the university would like to adopt, if funded?
- All terrific and important operational security topics, but NONE can be part of your presentation to the board: it would take too long to cover even just one such topic.
- Mr. Fail Boat says, "Ah ooh gah... now departing, pier #1..."

OR... Do You Talk About "GRC"?

- Governance: *someone's* in charge of cybersecurity. There's a firm hand on the security tiller, and *oversight.* An "adult" is paying attention to what's going on in that area.
- Risk: We're "business savvy." We "get it" that fixing stuff costs money. We're not going to try to fix "everything," or buy solutions just because they're technically "cool," we're only going to fix the security stuff that's really a problem, and only when it makes financial sense. There's a responsible hand on the institutional checkbook.
- Compliance: If the law says we have to do something (particularly ifthere are consequences if we don't), we know what we're supposed to do and we're going to do it, we're not ignoring specific legal requirements. Audits aren't going to come back full of embarrassing findings.
- GRC == a well-tailored approach for *that* audience.

GRC Uptake Is Also Driven By "The Cloud"

- If you're outsourcing facilities and applications to third parties, your ability to even *attempt* to do technical security may be disappearing (you may simply not have the access you need to do technical security any more – e.g., you may not be allowed to check data center physical security, sniff traffic or actively scan the systems that are hosting your cloud based applications). So what's left?
- Governance decisions about what applications will move to the cloud and who the organization will use and trust.
- Risk management via SLAs and contractually enforced protective mechanisms
- Audit reports attesting to compliance with all applicable standards and requirements...
- If you're going to the cloud, you *ARE* going toward GRC.

Contrasting Approaches: Awareness & Training

- Operational security approach: many of the vulnerabilities we see are associated with badly written web applications. Let's bring in some experts in the OWASP Top 10 web security issues, and ensure our developers know how to avoid accidentally allowing those bugs into the applications that they write. [in-depth technical training, selectively targeted, driven by observed local vulnerabilities]
- The GRC approach: The security framework we've adopted requires us to do annual security awareness training for our community, and if we don't do that training, we won't be in compliance – and some users may end up getting phished. Let's buy SANS "Securing the Human" training for end users. It not only ensures we're compliant, "it offers training that changes behaviors and reduces risk."
- **Non-rhetorical question:** which approach is "better?"

Competition for Resources

- In an ideal world, we'd want BOTH operational/technical security AND GRC-based approaches.
- Unfortunately, in the real world, you've got finite budget and personnel slots. If you buy more OpSec people, you have less money left for GRC people, and vice-versa.
- Note that GRC has an "unfair" advantage in this competition: GRC-oriented people have direct access to senior leadership, and "they talk the language of those that hold the purse strings:" we've got a plan, there's an adult in charge, we're business savvy, and if you do what we tell you, you won't end up embarrassed.
- But "beating" OpSec people and successfully pushing GRC-based approaches may be a Pyrrhic victory (a victory with such a terrible cost that it is tantamount to defeat).

100% Compliant, But Also 100% P0n3d?

- You've made some hard choices, and allocated your limited resources. You're 100% compliant with all applicable requirements. You've assessed the risks your school faces, and your governance committee has signed off on a plan that follows a well known security framework. Unfortunately, doing so has meant that you didn't have much money (or many staff slots) left for operational/technical cyber security.
- Late one Friday night you're contacted by a reporter from CNN... the "unthinkable" has happened and a major breach has occurred, exploiting a technical vulnerability that you knew about, but which was deemed "low risk...."

[Pinkie Pie graphic from http://mlp.wikia.com/wiki/Pinkie_Pie , CC-BY-SA]

What Will *You* Say/Do?

- We can talk about the hypothetical case from the preceding slide, or about decisions in real life (someday, the two may even be exactly the same, unfortunately)

- You can fully meet all expectations of a GRC-oriented approach, and STILL end up experiencing a breach.

- If you'd spent more of your resources on technical/ operational security, you might not have experienced a breach -- but then again, investing in technical/ operational security also might make no difference.

- What will YOU say/do?