Cyber Risk
#whoami

Josh Sokol

- Former OWASP Foundation Global Board Member (https://www.owasp.org)
- Creator of SimpleRisk (https://www.simplerisk.com)

Twitter: @joshsokol
Blog: http://www.webadminblog.com
Today’s Agenda:

- Market drivers for cyber risk governance
- Key stakeholders in assurance and reporting
- The case for IA’s leadership in cyber
- Available methods and standards

Note: I wasn’t the original speaker for these topics. I’m not in IA. I’m basically the CISO. Don’t hate me if I get it wrong. ;-)
Market Drivers
For Cyber Risk Governance
RISK

The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).
Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.
Such a **risk** could materialize in the following ways:

**Deliberate**
and unauthorized breaches of security to gain access to information systems for the purposes of espionage, extortion or embarrassment.

**Unintentional**
or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed

**Operational**
IT risks due to poor systems integrity or other factors

**Note:** Organizations should not only be concerned with these things happening to them directly, but should also consider the effects should key companies in their supply chain or other parts of their extended enterprise be affected.
In 2017, what were the odds…

- Getting struck by lightning? 1 in 960,000
- Dating a millionaire? 1 in 220
- Experiencing a data breach? 1 in 4

(Global average 28%)
Biggest data breaches of the 21st century:

- 2017 – Equifax (143m records)
- 2016 – Adult Friend Finder (412.2m records)
- 2015 – Anthem (78.8m records)
- 2014 - eBay (145m records), JP Morgan Chase (76m records), Home Depot (56m records)
- 2013 – Yahoo (3b records), Target (110m records), Adobe (38m records)
- 2012 – US OPM (22m records)
- 2011 – Sony PSN (77m records, RSA (40m records)
- 2009 – Heartland Payment Systems (134m records)
- 2006 – TJX Companies (94m records)
The average total cost of a data breach was $3.62 million in 2017.

The global average cost was $141 per record.
Small businesses are not immune to cyber risks – there is growing evidence that criminals are targeting the less protected organizations.
Cyber Security Regulation

**NIST 800-171**
Supply-chain security for every government contractor handling Controlled Unclassified Information (CUI).

**GDPR**
Mandated to strengthen and unify the protection of EU citizen data for every company which stores or processes this data.

**PCI DSS**
Security standards for any organization which stores or processes payment card data.

**State Breach Notification**
47/50 states (+DC) have cybersecurity compliance requirements for organizations to notify states about security breaches of consumer data.

**HIPAA**
Provides data privacy and security provisions for safeguarding medical information.

**Many more...**
DFARS, FFIEC-IT handbook, FERC, NERC, etc.
Key Stakeholders

In Assurance and Reporting
Key Stakeholders in assurance and reporting:

first
Audit Committee
Maintain board level corporate objectives and provide guidance on corporate governance.

second
Internal Audit
Reports to Audit Committee in order to provide unbiased assurance statements by risk, department, or process.

third
IT Audit
Validates that organizational controls provided by Information Security are performing as expected.

last
Information Security
Defines organizational controls for risk mitigation and utilizes metrics in order to measure their effectiveness.

Other key stakeholders include: Management, Regulators, External Audit, etc.
The Case for IA’s Leadership in Cyber
I’m not sure “Leadership” is the right word here. Maybe “Participation” is a better way to describe the role Internal Audit should play in Cyber Risk assurance. At a minimum, IA needs to be aware of the role cyber risk plays in an organization because the Board will be asking about it and they need to provide independent guidance on it.
Cyber security needs to be a **collaborative effort:**

- IA, IT Audit, and Information Security define the organization’s controls based on a combination of best practices and regulatory requirements.
- Information Security handles daily operational responsibilities.
- Information Security captures metrics and reports on tool effectiveness and risk trends.
- IT Audit is responsible for routine testing of controls to validate controls are operating as expected.
- Internal Audit should be leveraged to provide testing independence and garner support for security initiatives at the Board level.

**Note:** EY (External Auditor) has been asking questions about our cybersecurity processes since ~2015. Historically, their inquiries have been pretty remedial, but I expect them to get more and more detailed over time based on guidance from the PCAOB.
Available Methods and Standards
Which **standards** you choose depends on how much **time** you have and any **regulatory requirements**:

- **ISO 27000** – The gold standard of security compliance. Have to purchase. Can have your organization ISO 27k certified. Maximum assurance for maximum effort.


- **AICPA Cybersecurity Risk Management Framework** – Guidelines on how to examine and report on an organization’s cybersecurity risk management program.
There's basically **two ways to do it:**

**Required Frameworks**
Take every regulation that applies to you and grab the framework for it. Manage each control individually. Do your compliance testing across each individual framework.

- **PRO:** Tailored to exactly what your org needs and nothing more.
- **CON:** You have to test everything individually.

**Common Control Frameworks**
Use a proprietary set of controls that is mapped across multiple frameworks. Do your compliance testing across the common control framework.

- **PRO:** Reduced audit effort from testing a common control set.
- **CON:** Difficult to prove an attestation point with a set of proprietary controls.
Tools:

- **LOW END**: Most of the audits that I’ve seen use a combination of spreadsheets and wikis to track the audit results.

- **HIGH END**: Governance, Risk, and Compliance (GRC) tools.
● Free and open source tool to provide Governance, Risk Management, and Compliance capabilities for organizations big and small.
● Way more powerful than spreadsheets and wikis.
● Way cheaper and less complicated than commercial GRC tools.
Demo
Thanks!

Any questions?

@joshsokol
josh@simplerisk.com
https://www.simplerisk.com