BRIDGING THE GAP:
MEASURING & COMMUNICATING RISK ACROSS THE ENTERPRISE
GROWTH IS BEING FUELED BY TECHNOLOGY

Growth is the highest priority

Technology initiatives are second priority

54%

25%

Gartner, "2015 CEO and Senior Executive Survey: Committing to Digital" (April 2015 / September 2016) [G00274031]
BUT RISK MANAGEMENT IS FALLING BEHIND

New risks challenge the business 77%

Risk management is falling behind 65%

Agility is increasingly important 83%

Gartner, "2015 CEO and Senior Executive Survey: Committing to Digital" (April 2015 / September 2016) [G00274031]
HOW IS SECURITY COMING ALONG?

- 70% Compromised in the last year[^1]
- 90% Are unsatisfied with response speed[^2]
- 80% CISO’s re-thinking strategy in next 12-18 months[^3]

[^1]: RSA Cybersecurity Poverty Index 2016
[^2]: RSA Threat Detection Effectiveness Survey 2016
[^3]: RSA estimate
MANAGING RISK IS A BUSINESS AND A TECHNOLOGY CHALLENGE

Magnitude of risk increasing

Velocity of risk increasing

Risk Complexity increasing
TECHNOLOGY RISK

• What is the important data?
• Where is the important data?
• What are the most critical applications?
• How important is this part of the infrastructure?
• What does this security event impact?
• Where are we vulnerable?
• Who are the 3rd parties the business rely on?
• What happens if IT services are disrupted?

BUSINESS RISK

• What part of the business strategy is the most critical?
• Where are our biggest risk areas?
• What is our risk appetite and tolerance?
• What are our regulatory obligations?
• What are the most valuable pieces of our business?
• How bad could it be?
• Are we effectively managing our risks to achieve our objectives?
METRICS AND “THE GAP”
WHY BOTHER?

The future is coming – can you hear it?

“Eventually, the insurance industry will subsume the computer security industry.”

− “Not that insurance companies will start marketing security products, but rather that the kind of firewall you use – along with the kind of authentication scheme you use, the kind of operating system you use, and the kind of network monitoring scheme you use – will be strongly influenced by the constraints of insurance.” Bruce Schneier

Will a savvy understanding of the metrics of your internal environment become even more important as this happens?

WHY BOTHER?

Obtain insight

Speak to the business in its own language

- The security program has measurable business value

Objectively demonstrate security objectives are being met

Justify new investments

Improve!

"Technical Metrics Aren't Enough: 10 Strategic Security Measures" (Julia Allen & Lisa Young, 2014)

POOR METRICS

Easy to collect, but not very actionable
- Operational metrics ≠ Business-centric metrics

Examples of what NOT to measure
- Spam emails received
- Virus infection attempts blocked
- Technical security vulnerabilities resolved
- Failed logins

We tend to measure what we can’t control

PRAGMATIC Security Metrics (W. Krog Brotby & Gary Hinson, 2013)
POOR METRICS

Figure 1. Perimeter Security Incidents (January 2007)

Source: Gartner (September 2007)

"Toolkit Best Practices: Selecting Security Metrics" (Jeffrey Wheatman/Gartner, 2007)
POOR METRICS

Subjectively measured

Inconsistently measured

Costly to gather

May not be “metrics” at all

May not be built for your true audience

Security Metrics (Andrew Jaquith, 2007)
KNOW YOUR AUDIENCE

Create a common language between the Business and Security

CISOs are the most influential security-focused consultants to the Business – or rather, they *should* be

Metrics must reflect the role and the value that the Security organization plays in the Business strategy

“Don’t Bore Your Executives – Speak To Them In A Language That They Understand” (Ed Ferrara/Forrester, 2011);
cartoon licensed from Mark Dubowski
KNOW YOUR AUDIENCE

The “language” of Security is hard for the Business to fully understand
- Presentation skills are essential – practice!

Business leaders are challenged in communicating back to Security, too!
- Understand the goals/initiatives of the Business units

Communicating in a Business context
- Standard templates, communication tools + a taxonomy document

The Business finds it extremely difficult to identify its own risk appetite
- Consider scenarios and story-telling as tools

"Why Communication Fails: Five Reasons the Business Doesn’t Get Security’s Message" (Jeffrey Wheatman/Gartner, 2011)
ABSTRACT OUT
THE TECHNOLOGY & OPERATIONAL METRICS

Number of times we were “attacked” last month

Number of unpatched vulnerabilities

Number of unpatched critical vulnerabilities against critical systems

Percentage of unpatched critical vulnerabilities against critical systems

Number of days it takes to patch critical systems with critical patches

Number of days it takes to patch systems supporting the manufacturing line in Kuala Lumpur with critical patches

“No One Cares About Your Security Metrics and You are to Blame” (Paul Proctor, 2013)
WHAT MAKES A “GOOD” METRIC?

The source of the problem, or necessary actions to take, are clear when the metric goes up, down, flat or off-target.

Actionable

People in the organization recognize what the metric means.

Common interpretation

The data can be acquired with modest effort from a source that people trust.

Accessible, creditable data

How the metric is generated is shared and easy to understand.

Transparent, simple calculation

The perfect metric

“Choosing the Right Metric” (Zach Gemignani, 2007)
http://www.juiceanalytics.com/writing/choosing-right-metric
WHAT MAKES A “GOOD” METRIC?

“The primary goal of metrics is to quantify data to facilitate insight.” Andrew Jaquith

A good metric is:

- Consistently measured
- Cheap to gather
- Expressed as cardinal number or percentage
- Expressed using at least one unit of measure
- Contextually specific
WHAT MAKES A “GOOD” METRIC?

Quantifiable information
- Ability to compare and trend

Readily obtainable

Consistent and repeatable processes only

Track relevant performance trends over time

Point to improvement actions

“Performance Measurement Guide for Information Security” (Elizabeth Chew et al., 2008)
EXAMPLE

- Number of orphaned information assets without an owner

*Be thinking about...*

- Do you know where all of your information assets reside?
- Do you explicitly assign / name owners for assets? How does this process work today?
- Do all of your information assets need an owner?
- How do you know if a designated/responsible owner is still on the payroll?

*PRAGMATIC Security Metrics* (W. Krag Brotby & Gary Hinson, 2013)
Percentage of third-party users whose privileges were reviewed this reporting period

Be thinking about...

- Do you understand your potential third-party vendor areas of risk?
- Do you know which external vendors have accounts associated with your assets?
- Are there any assets where electronic communication to/from external vendors (including system-to-system access) is simply not allowed?

https://net.educause.edu/ir/library/pdf/CSD3661.pdf [via Jaquith]
CAVEATS

Don’t blindly accept your vendor’s proffered metrics.

- “We tend to overvalue the things we can measure and undervalue the things we cannot.” John Hayes

Metrics should be actionable!

- “If a measurement matters at all, it is because it must have some conceivable effect on decisions and behaviour. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value.” Douglas W. Hubbard
IS THERE ONLY ONE INTERPRETATION?

“More than Mitigating Risk: The Future of Co-Creating Value with Stakeholders” (Tara Addis, 2011)
MORE ON METRICS

The one place to start for a foundational background (strategic)

Or, skip to here for content specific to risk management and information security (tactical)
KNOW WHICH RISK IS WORTH TAKING

RSA

ARCHER® SUITE