Enterprise Security Governance and Strategic Planning

*What is the latest thinking to address the cybersecurity challenge?*

Earl Crane, PhD
Earl Crane is the CEO of Emergent Network Defense, providing a Digital Risk Management solution to help organizations, governments, and financial institutions “secure what matters” through a biological ant-based swarming artificial intelligence.

• Previously he was the Director for Federal Cybersecurity Policy at the White House National Security Council.

• Prior to his recruitment to the White House staff, Dr. Crane was the Director of Cybersecurity Strategy and the Chief Information Security Architect at the Department of Homeland Security.

• Most recently, he was a Director with Promontory Financial Group, a strategy, risk management, and regulatory compliance consulting firm.

• Elected to (ISC)2 Board of Directors for 2018

Earl Crane, PhD, CISSP
CEO, Emergent Network Defense
CRANE@ANDREW.CMU.EDU
EARL@ENDSECURITY.COM

Ph.D. George Washington University in emergent network defense (2013)
If you get one thing from today...

Capturing and governing your organization’s cyber risk appetite is crucial to its survival.

“It looks like you have no appetite for risk”
Cyber Risk Management Model

Impact
“How bad could it be?”

Scenario Exposure
“What could happen?”

Key Metrics
“What needs to change?”

Relative to Appetite
“Is it acceptable to the organization?”
War of 1812

- Secretary of War John Armstrong refused to take warnings about a British threat seriously
- DC was a small, backwater town, built on a swamp, with no perceivable tactical military advantage.

His reply when pressed by General Van Ness was,

‘Oh yes by God, the British will strike somewhere: but not here! What the devil will they do here?... no, no! Baltimore is the place, sir; that is of so much more consequence.’”
Why wait for the house to burn down?
“...the folks who did this didn’t just steal practically everything from the house; they burned the house down. They took our data. Then they wiped stuff off our computers. And then they destroyed our servers and our computers.”

Michael Lynton,
CEO Sony Pictures Entertainment
Moving Beyond Cybersecurity

$100bn in losses

“We should have seen this coming.”

Digital Exposures
Executive Attention

Increased Focus on Cyber Risk Management

“Current cybersecurity strategies fail, stakeholders lack education, and cybersecurity failure costs are equivalent to 1/3 of US GDP worth of information stolen each year.”
– National Association of Corporate Directors, Cyber-Risk Oversight: A Focus on ERM and C-Suite to Boardroom Collaboration, April 2016

61% of CEOs cited Cyber Threats as a key risk in 2016.

“The key is ignoring the press and understanding your own top risks. The top risks that sell newspapers may be different than the risks that could kill your bank.”

“Cybersecurity routinely makes the top 5 list of CIO concerns. Increasingly, instead of fixed solutions to security issues, artificial intelligence is being incorporated into IT security product to dynamically investigate and respond to unique and emergent security breaches on the fly.”
– The enterprise technologies to watch in 2016, May 29, 2016
External Expectations

“Organizations will learn to live with **acceptable levels of digital risk** as business units innovate to discover **what security they need and what they can afford.**”
– Gartner VP and Analyst Paul Proctor, June 23, 2016

“Cyber is going to continue to be a more prevalent risk issue. While it started off more in the IT world, it has become a board issue, and the C-suite needs to deal with the complexities of cyber risk.”
– Marsh Global CEO Peter Zaffino, March 31, 2016

“Risk managers are asking for a comprehensive strategy that helps them assess their cyber and data privacy risk, incorporates appropriate loss control services to mitigate losses before they happen, provides access to post breach services to assist them in the event of a breach, and offers higher limits to meet their coverage needs.”
– Toby Merrill, Global Cyber Risk Practice ACE Group, September, 2015

“If we were to believe that a bank is ill-prepared to withstand a cyberattack, we could downgrade the bank before an actual attack.”
– Standard and Poor’s Capital, September 28, 2015
Heightened Regulatory Expectations

**OMB**

Management’s responsibility is to develop and maintain effective internal control that is consistent with its established risk appetite and risk tolerance levels.


**FFIEC**

The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.

Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.

– Cybersecurity Assessment Tool, June 2015

**CFTC**

“[Cybersecurity] is perhaps the single most important new risk to financial stability ... We require clearinghouses, exchanges, and other market infrastructures to implement safeguards, and we are focusing on this issue in our examinations. ... we want to make sure the board of directors and top management are making this a priority.”

– Chairman Massad, January 2015

**FRB**

The Federal Reserve requires the financial institutions it regulates to develop and maintain effective information security programs that are tailored to the complexity of each institution's operations and that include steps to protect the security and confidentiality of customer information.

– Governor Tarullo, February 2014
Why do we need strategy?
Three lines of defense

First Line
- Risk Ownership
- Operational management
  - Day-to-day tempo
  - Provide strategy for controls
  - Identify, assess, control, and mitigate risks
  - Security is designed into the systems

Second Line
- Risk Oversight
- Work closely with first line
  - Supporting management policies, defining roles and responsibilities, and setting goals for implementation
  - Providing risk management frameworks
  - Identifying known and emerging issues
  - Identifying shifts in the organization’s implicit risk appetite
  - Assisting management in developing processes and controls to manage risks and issues

Third Line
- Risk Assurance
- Independent assurance function
  - Periodic audit and review, including operational efficacy, safeguarding, reporting, and compliance
  - Report sufficiently high in the organization and to governing body
A different mindset at the second line

Third Line of Defense
Audit and Review
Independent Assurance:
Senior Management & External Reporting

Second Line of Defense
Risk Management
Risk Oversight:
Monitor, Identify Emerging Issues, Identify Risk Appetite Shifts

First Line of Defense
Operational Management,
Risk Ownership:
Control Implementation

Validation of First Line operations, Second line effectiveness
Effective challenge of risk functions across the enterprise

Traditionally manual processes and tools, periodic consultants, and subjective assessments
AI beginning to help with context

Solutions are tactical and point-focused in nature
Rigid compliance frameworks
Risk is not a game of “Whack Attack”
It’s a Game of “What Ifs?”

“Fight every battle everywhere, always in your mind...Every possible series of events is happening all at once. Live that way and nothing will surprise you. Everything that happens will be something that you’ve seen before.”
How to think about risk at the second line

- **Relative to Appetite**: “Are we within our comfort zone?”
- **Impact to Business**: “What can hurt the business?”
- **Scenario Exposures**: “What incidents might create losses?”
- **Key Risk Indicators**: “Should we be nervous about the data?”
Digital Risk Questions

What Matters?

What are your Risk Categories and Appetite?

What keeps you up at night?
What loss scenarios have happened?
What might expose us in the future?

What data do you have?
What makes you nervous?
Cyber Risk Management Model

1. Scenario Exposure: “What could happen?”
2. Impact: “How bad could it be?”
3. Key Metrics: “What needs to change?”
4. Relative to Appetite: “Is it acceptable to the organization?”

RISK

CHIEF INFORMATION SECURITY OFFICER

© Emergent Network Defense, Inc.
What Matters?

As leaders and executives ask yourself:

- What is the risk culture?
- What are the “crown jewels”?
- What would the business impact be if you lost control?
Risk Categories

• You are the owner/executive of the risk catalog. What are the top risks for your organization?
  • Capital, Assets, Management, Earnings, Liquidity, Sensitivity to markets (CAMELS)
  • BASEL III (Capital, Leverage Position, Liquidity)
  • Credit, Liquidity, Market, Profit, Systemic, Settlement, Operational (ERM - Banking)
  • Audit, Management, Development and Acquisition, Support and Delivery (AMDS)
  • Reputational, Strategic, Compliance, Agility, Business, Technology, Culture, Environmental, Others

• What risk categories represent your ”crown jewels”? 
Risk Appetite

A standard approach to risk appetite is to think about it like a point on a line

- Risk Appetite: The amount of risk the firm chooses to take
- Risk Capacity: The total amount of risk the firm can withstand
- Risk Tolerance: Deviation an organization is willing to accept

(Note: While useful as a thought exercise, this approach is less helpful when later discussing loss probability)
Qualitative vs. Quantitative Appetite?

Risk Appetite has traditionally been thought of as a qualitative scale (Low, Moderate, or High). However, this is insufficient for wise management decisions. It leads to subjective and uninformative constructs like the Risk Heatmap or Stoplight Charts.
Risk Acceptance on a Probability Curve

- **Appetite/High Acceptance:** Scenarios that are the cost of doing business.
- **Acceptance Drops:** Scenarios that are bearable but not preferable.
- **Very Low Acceptance:** Scenarios that present hardship to the business.
- **Capacity/No-Acceptance:** Scenarios are existential threat to the business.
Comparing Appetites

![Graph showing the probability of exceeding a loss for different amounts. The x-axis represents the loss in dollars, and the y-axis represents the probability of exceeding that loss as a percentage. The graph includes data points for $100,000.00 at 100%, $250,000.00 at 80%, $750,000.00 at 50%, and $55,000,000.00 at 0%. ]
The Objective: To compare appetite to a risk projection

Appetite

$150,000.00
100%

$450,000.00
80%

$750,000.00
40%

$50,000,000.00
0%

Projection

$100,000.00
100%

$250,000.00
80%

$750,000.00
50%

$60,000,000.00
1%

Probability of Exceeding Loss

Loss

Low
Mod
High
Critical
Where does Risk Appetite come from?

Cyber Knowledge
“How do we protect it?”

Business Wisdom
“What Matters?”

Risk Knowledge
“What is the business impact?”

Operational Telemetry
“How do we know what we know?”

Cyber Risk
“How much is too much?”
Capacity Management

Consider:

• How bad can it get?
• How do you tell the story?
• To whom do you tell it?

Get inside the heads of the business:

• Impactful storytelling
• Culture of the organization
Poor Examples of Risk Appetite

• “We have zero tolerance for fraud” – Fraud can not be eliminated

• “There is a low appetite for cyber losses” – The term “low” is vague and needs to be quantified

• “The cyber risk appetite of the organization is medium” – Unclear how this is executed or the impact of this statement

• “Our cyber risk appetite is bounded by the annual value of cyber risk losses. We do not have an appetite for cyber risk losses that exceed $20MM for the year.” – Confusing appetite for loss with a tolerance threshold

• “The cyber risk appetite of the organization is defined by the cyber risk loss value using a 99.5% confidence level on our statistical loss distribution”. – Good quantification but unclear around what it means.

Association of Foreign Banks (AFB)
Risk Appetite Concepts

- Should be set in both quantitative and qualitative terms:
- Should consider the risk-reward dynamic;
- Have clear trigger points, actions and escalation processes;
- Have clearly described monitoring or arrangements and appropriate ownership thereof;
- Be formally set and approved by the appropriate governance body and appropriately disseminated down/translated for lower levels;
- Can be set at various levels. e.g. Board, region, entity, business line, department;
- Have clear ownership at the respective levels;
- Be embedded/used by the business;
- Be expressed through a suite of measures rather than just one 'measure' or parameter (e.g. just losses or just Key Risk Indicators):
- Be simple to understand;
- Be appropriately documented and reviewed on a periodic basis.

Association of Foreign Banks (AFB)
Characteristics of Effective Risk Appetite Statements:

- Directly links to the organization’s objectives;
- Is stated precisely enough that it can be communicated throughout the organization, effectively monitored, and adjusted over time;
- Helps with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risks.
Based on the discussion, the following assertions should part of Cyber Risk Appetite:

**Position** – Establishes what is an acceptable/unacceptable state, and how much.

**Value** – Establishes the value of what is being protected and ties into corporate values/objectives.

**Metric** – Key performance/risk indicators to monitor tolerance of risk to the desired condition.

**Plan** – Predetermined escalation and correction to adjust risk.
Appetite Discovery

<table>
<thead>
<tr>
<th>Qualitative Statement</th>
<th>Quantitative Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Value</td>
</tr>
<tr>
<td>“Company has a ______ appetite for ______,”</td>
<td>”because…”</td>
</tr>
</tbody>
</table>

The first half of risk appetite is a documented recognition of the types of risks the enterprise wishes to embrace or avoid, by how much, and tied to corporate value.

The second outlines the key risk indicators to be tracked, their thresholds, and actions (escalation or remediation) if they exceed.
Motivate the business to listen.
Tell a better story.

June 21, 2017 – Fmr. DHS Sec Jeh Johnson testifying on the struggle to accept DHS assistance.

“Prior to the election, encouraging the horses to come to the water had to be the primary objective...

My staff and I repeatedly encouraged state and local election officials to seek our cybersecurity assistance.”
Progression of Risk Management Approaches

Why has it been hard to motivate business?

Cybersecurity traditionally focuses on only one dimension of risk.

- **Targets (Assets)**
  - What do you have?
  - What are you protecting?

- **Vulnerability**
  - Detect and close every vulnerability.
  - Maintain compliance.

- **Threat Actors**
  - Understand completely your adversary.
Example Scenario: A malicious actor takes advantage of a vulnerability in phishing defense capability that results in data leak of operational data that has a HIGH reputational and legal Impact.

Potential Business Impacts come from:
- Historical Losses
- Peer Losses
- Financial Business Models
- “Calibrated” Experts

Potential business impact range $10K to $500K or Low, Mod, High, V. High (historical incidents or calibrated estimation.)
Assessing a Loss Exposure Scenario

Ask yourself “what would make me nervous about this scenario?” and look at each object through several data sources.

A scenario with several overly “nervous” objects is likely to be highly exposed.

<table>
<thead>
<tr>
<th>Actors</th>
<th>Vulnerabilities</th>
<th>Targets</th>
<th>Consequences</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untrusted External</td>
<td>Phishing</td>
<td>Operational Data</td>
<td>Data Leak</td>
<td>Reputation &amp; Legal</td>
</tr>
</tbody>
</table>

- **Untrusted External**
  - Twitter Chatter
  - Risky Day Calendar
  - Blacklisted Traffic

- **Phishing**
  - Spam Filters
  - Employee “Clickiness”

- **Operational Data**
  - DLP Alerts
  - Asset Exposures

- **Data Leak**
  - Conf

- **Reputation & Legal**
  - Rep
  - Integ
  - Legal

Potential business impact range:
- $10K to $500K
- Low, Mod, High, V. High

(historical incidents or calibrated estimation.)
Many Questions, Many Data Sources

Metrics answer “should I be concerned about this?” “Nervousness” is a normalized scale using data against expected thresholds.

Even a lack of data is helpful with this approach. It can identify new tools or allow for reprioritization.
“We turned to other scenarios” the Russians might attempt, said Michael Daniel, who was cybersecurity coordinator at the White House, “such as disrupting the voter rolls, deleting every 10th voter [from registries] or flipping two digits in everybody’s address.”
Composing New Loss Exposure Scenarios

Reusing objects allows for many more scenarios
Thank you

Secure what Matters

Earl Crane

crane@andrew.cmu.edu
earl@endsecurity.com