Managing Cybersecurity Risk

Top to Bottom

Bruce Miller, PhD

Navair Cybersecurity Risk Assessor

Head, RDT&E Infrastructure (541000D/E)

11 Feb 2019

Organizational Cybersecurity

Focus Areas

- Organizational executive leadership
- Senior cybersecurity leadership
- Cybersecurity professionals and
  Organizational insiders
- Use case: shadow IT

"Cybersecurity is everyone's responsibility"

Executive Leadership

Executive Leadership

Cybersecurity: a key component of organizational governance

- Uncontroversial as a executive level responsibility
  - Validate alignment of cybersecurity and business objectives
  - Endorse risk management strategy
  - Actively support, monitor, and guide strategy
  - Assure sufficient resource management

Cybersecurity is a business decision, not an IT decision

Executive Challenges

Little agreement about how cybersecurity is best achieved

Critical factors to success span the organization

- Human resources
- Organizational structure
- Top management commitment
- Strategy (defined and implemented)
- Organizational culture

Top risk: Over-simplification through focus on rigid compliance

Senior Cybersecurity Leadership

Senior Cybersecurity leadership

- Responsibility highlights
  - Align cybersecurity strategy to organizational strategy
  - Long and near term prioritization
  - Development and ownership of policies
    - Includes: Security Education, Training, and Awareness
  - Manage resources
  - Build metrics, monitor, and report effectiveness
  - Assure alignment of intent and reality

- And challenges…
  - It is the same list
  - Best practices rooted in General Deterrence Theory
    - Cybersecurity is more complex

Complexity of the Challenge

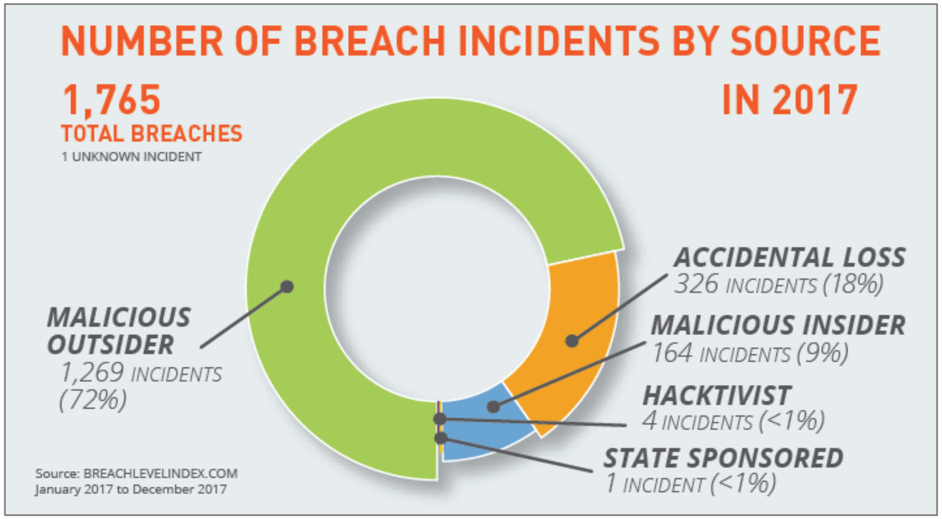
Breaches in Confidentiality

Outsider vs. Insider

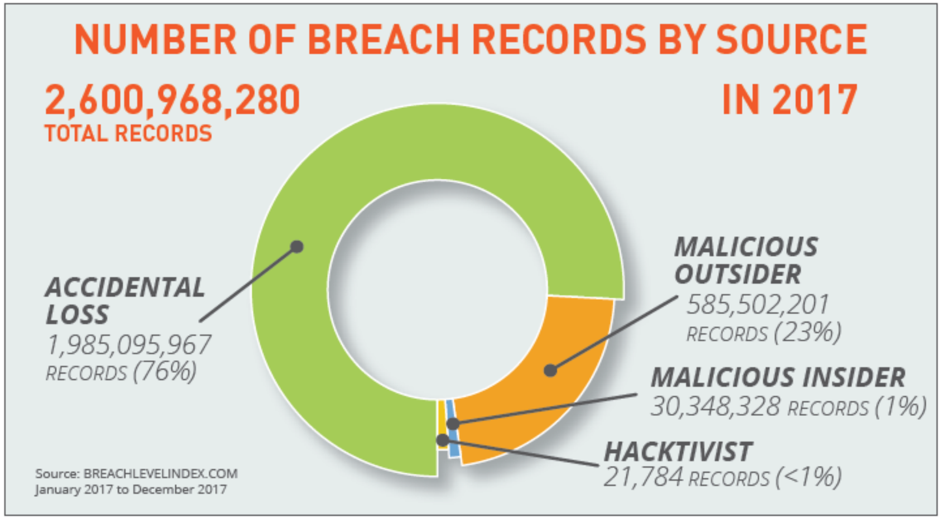
- Outsider 4x more frequent
- Insider **18x more impactful**

And this is not the whole story…

- Publically acknowledged data
- Mixes intent and outcome
- Limited to confidentiality
- Omits losses related to
  - Integrity
  - Availability



Source: BREACHLEVELINDEX.COM
January 2017 to December 2017



Source: BREACHLEVELINDEX.COM
January 2017 to December 2017

“Security” vs. “Protection”

Inherently different things

- Impact of failing to recognize the difference
  - Over-emphasis on confidentiality
  - Deviation from strategic priorities
  - Loss of information value

- Not all information has the same value
  - We inherently know this
  - Conflict between knowing and doing

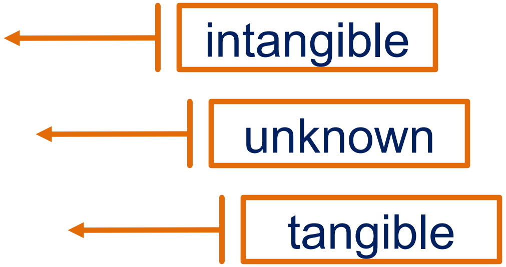
Strategic vs. Tactical

Cybersecurity Risk Management

Risk = Probability * Consequence

- Cybersecurity context: limited practical value
  - Probability and consequence are indeterminate
  - Cost vs. benefit is inherently relative
  - Risk perception is highly sensitive to communication

- Implementation of every control has
  - benefit
  - failure rate
  - cost



intangible

unknown

tangible

Cybersecurity Professionals and Organizational Insiders

The Workforce and Cybersecurity

Constantly make decisions that affect cybersecurity

High Variability

- Level of responsibility for cybersecurity
- Knowledge, skill, and abilities
- Approaches to conflict resolution
    - Meaning: reconciling competing priorities

Challenges are not limited to policy compliance

- Development
- Implementation
- Monitoring

Broad Scope of Insider Threat

Not just accidents :: Inherently risk management

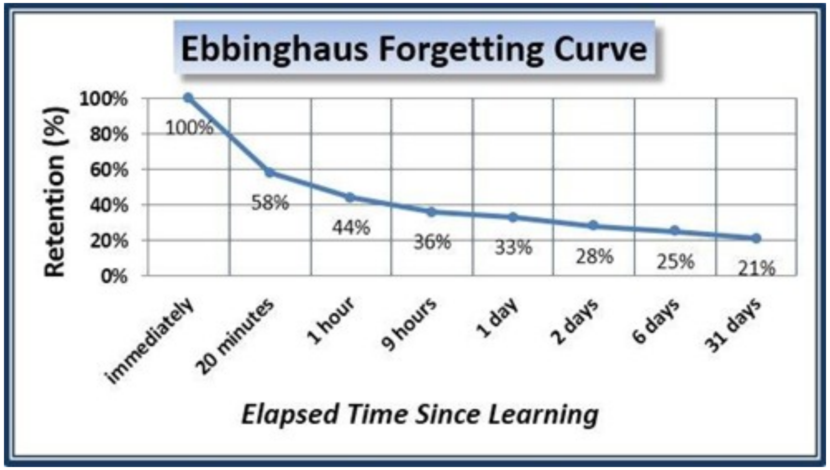
- Drivers of Risk Acceptance vs. Avoidance
  - Theories
    - General Deterrence Theory
    - Prospect Theory
    - Neutralization Theory
  - Influential Perception Attributes
    - Optimism bias:
      - Bias due to belief that risks are improbable
    - Availability heuristic:
      - Bias due to the ease of recalling a relevant example

Insider threat is rooted in an organization’s decision-making strategy

Security Education, Training, and Awareness

- Industry best practice: More training on policies and consequences

- What works
  - In person with someone you know, trust, and respect
  - Referencing incidents relevant to local environment
  - Focused on ethics and benefits
  - Timely
- What does not work
  - Negative framing
    - Prohibitions
    - Threats
    - Sanctions
  - General fear, uncertainty, and doubt
  - Computer-based training *



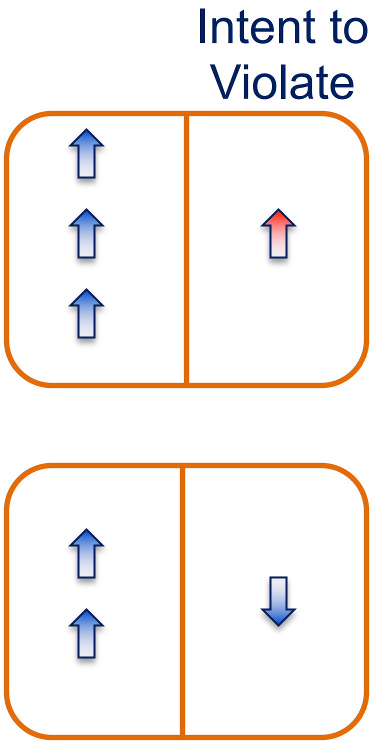
Cybersecurity knowledge is most often learned by asking someone nearby in the moment

Influence of Expertise

Higher expertise does not correlate to lower policy violations when neutralizing logic is a factor.

Intent to violate correlates:

- Positively
  - Cybersecurity and IT expertise
  - Level of education
  - Gender (male)
- Negatively
  - Work experience
  - Age



SETA as a best practice is not wrong; just incomplete

Use case: Shadow IT

Shadow IT (noun):

- Any hardware, software, or services built, introduced, and/or used to work without explicit approval or knowledge of the organization's IT management.

- The voluntary use of any IT resource violating IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization.

- A form of decentralized computing implemented by individuals, workgroups or whole business units, to include:
  - Unapproved services
  - Self-made solutions
  - Self-installed software
  - Self-acquired IT

Shadow IT is a Choice

- Born out of frustration and the decision to alleviate the situation by any means feasible

- Enabled by technology consumerization
  - Cost of small-scale/ entry-level IT
  - Low skill required to “make it work”
  - Cloud, containerization, x as a service

- Response to organizational IT systems
  - Inefficient
  - Inadequate
  - Malfunctioning

Not an End User Problem

Use of Shadow IT is rooted in an organization’s decision-making strategy

- Fails to acknowledge
  - Complexity of professional IT capabilities
  - Negative impact on those responsible for IT service
  - Criticality of cybersecurity as a national security priority
- Highly sensitive to
  - Personal knowledge and judgement
  - Personal conflict resolution motivation
  - Optimism bias (belief that risks are improbable)
  - Availability heuristic (ease of recalling a relevant example)
- Innovation and problem solving occurs at all levels
  - Strategies re-applied from technical issues to organizational issues

So long as organizational IT is perceived to be a “problem,”
Shadow IT will exist

Addressing Negative Impact of Shadow IT

IT/ IA Challenges		C	I	A
Little to no IT equipment lifecycle maintenance			X	X
Low accountability of information flow		X	X	X
Low accountability of IT equipment		X		X
Insufficient disaster recovery and contingency planning			X	X
Reduced compatibility and commonality with other systems			X	X
Insufficient cybersecurity implementation to manage risk		X	X	X
Absence of IT and IA governance		X	X	X
Data at rest protecti				
Non-repudiation failu				
Least Privilege princ				
Separation of duties				
Need to know violati				
Defense in depth no				
Incident response di				

Program Management Challenges
Highest long-term cost for IT
Maximum unnecessary complexity
Inadequate data management
High process management risk
High risk of IT failure and significant permanent data loss
Increased risk of dead-end solutions
… This stuff does not run itself.

Excuse-Making as Conflict Resolution

- Occurs in the moment, before the decision to act
- Context-specific (explains apparent inconsistency)
- Most common excuses: speed, difficulty, knowledge

“Cyber security is too hard”

“I have to do it”

“I was told to go faster, this is faster”

“I know what I’m doing”

“Nothing will happen”

“Just this once”

“I was told to take risks”

“I have no other choice”

“It’s a stupid rule”

“I’m not a threat”

“They don’t really mean it”

“No one will get hurt”

“It is the ‘right’ thing to do”

“I’m doing it to support the organization”

Reducing Shadow IT Motivations

- Improve perceptions of organizational IT/ IA
  - Policies show a benefit / value
  - Absence of hindrances
  - Minimization of costs (schedule, productivity, funding)
  - Responsive technical support
  - Solutions acknowledge convenience
  - End user input is requested, received, and discussed

- Security culture reduces policy violations when
  - We feel accountable for actions
  - We receive disapproval of workgroup members

Cybersecurity: Top to Bottom

- A multi-faceted challenge
  - Intended to support organizational priorities
  - Rooted in risk management
  - Prone to oversimplification
  - Impacted by decisions at every level

While an individual may be held accountable, failed cybersecurity is an organizational problem.

“Cybersecurity is everyone’s responsibility”
Support it by promoting good decision-making strategies