How We Try to Address Cyber Risk

What is Cyber Risk?
- Definitions
- Who should be concerned?
- Key categories of cyber risk

Cyber Event Scenarios
- Information theft
- Property damage
- Environmental damage
- Computer systems damage

Risk Action Framework
- Quantifying my unique potential cyber impacts
- Risk transfer challenges and optimization
- Effective controls to minimize the risk

But how does it really work?
Metrics and Measuring

The wild, wild west of cybersecurity…

**THE GOOD**
- We’re getting better at this
- More research than ever before

**THE BAD**
- Uncertain evolution of security metrics

**AND THE UGLY**
- Lack of data leads to subjectivity and red/yellows/greens
Building a Better Measurement Program

- Not all measurement is good measurement
- Compliance can be your friend (yes, I just said that)
- Metrics, by their nature, will evolve as your data gets better
Managing Risk Management
Silos everywhere
Tearing Down the Walls
Linking security with operations and finance
Elevating Security Metrics

Security is not a stoplight!
But It’s Still **NO ROI**

- Even with new metrics, how do security professionals align with “risk” as defined by the CFO?
- What does “Mean-Time-to-Fix” have to do with quarterly projections?
- How much “less risk” will we have after we patch our systems this week?
Quantifying Cyber Exposure

Source: Measuring and Managing Information Risk
Mapping cyber risk to financial impacts

Move away from “Identify, Protect, Detect, Respond, and Recover” and embrace your inner accountant:

- First and third party damages
- ICS adds a new component of cyber impact with physical damages
- This may get mildly uncomfortable

Losses Due to Cyber Events (data breaches, destructive attacks, and other unauthorized access or use of your computer systems) can be categorized into these four quadrants.
Data Breach Example – Target, by the numbers

40 million credit cards +
70 million customer records stolen

$54 million: income to cyber criminals

$400 million: cost of replacing credit cards

$150 million: Target initial response cost

$1 billion: estimated ultimate cost to Target

140: number of active lawsuits against Target

2: Number of C-suite executives at Target who were fired

7: Number of Directors targeted by Institutional Shareholder Services for ouster, claiming failed duties to shareholders

*Important to watch because of unprecedented impact of Board and C-Suite and record-breaking damages. All data with black-market value is at risk.*
Cyber Loss Spectrum

This is well-worn territory

- What hits your budget during an incident?
- Focuses on mostly non-ICS categories like credit monitoring
- It’s easy to get these values

Financial Damages

1st Party Damages
(to your organization)

- **Response Costs**: forensics, notifications, credit monitoring, crisis management, public relations
- **Legal Expenses**: advice and defense
- **Revenue Losses**: from network or computer outages, including cloud
- **Cost of Restoring Lost Data**
- **Cyber Extortion Expenses**
- **Value of Stolen Intellectual Property** and associated revenue and market share losses

3rd Party Damages
(to others)

Tangible (Physical) Damages
3rd Party Entities May Seek to Recover:
- Consequential **Revenue Losses**
- **Restoration Expenses**
- **Legal Expenses**
- **Credit Monitoring Costs**

Cyber Loss Spectrum

What hits your customers or partners when an incident occurs? What do they need to pay for—and what are you on the hook to pay them?
Stuxnet  
Aurora  
BSI Steel Mill

<Insert Well Known ICS Security Example Here>
Cyber Loss Spectrum

Quantifying the destruction that may happen during a cybersecurity incident with ICS.

This could dwarf the estimates for “traditional” data breach quantification.

- **Mechanical breakdown** of your equipment
- Destruction or **damage to your facilities** or other property
- **Environmental** cleanup of your property
- **Lost revenues** from physical damage to your (or dependent) equipment or facilities (business interruption)
- **Bodily injury to your employees**
And it would impact your business partners, too, potentially. What would you be liable for?

- **Mechanical breakdown** of others’ equipment
- Destruction or **damage to others’** or other property
- **Environmental cleanup** of others’ property
- **Bodily injury** to others
A New Metric Emerges

Creating a balance sheet of cyber impacts based on *extreme, yet plausible* scenarios
Enter the topic I really want to talk to you about.
Cyber Insurance Timeline

1990
- Cyber coverages begin to appear

2000
- More robust electronic data exclusions
- Privacy Breach Liability Coverage
- Breach Regulatory Event Expense
- Network Business Interruption Information Asset Protection

2010
- P&C carriers strengthen exclusions, e.g. CL380
- New cyber coverages emerge
- Stuxnet

Events
- Ingram Micro v. American Guarantee & Liability
- CASB 1386 Breach Notification
- 46 State-level Notification Laws

Future?
Affirmative coverage in existing lines
Available Insurance

Widely Available Cyber Insurance

- ~60 Insurers
- Limits of up to $200 Million (or greater with some work)
- Specifics vary by carrier: triggers, cloud asset coverage, flexibility in service providers (read the policy)

Unavailable Coverage

Financial Damages

1st Party Damages (to your organization)

- **Response Costs:** forensics, notifications, credit monitoring, crisis management, public relations
- **Legal Expenses:** advice and defense
- **Revenue Losses:** from network or computer outages, including cloud
- **Cost of Restoring Lost Data**
- **Cyber Extortion Expenses**
- **Value of Stolen Intellectual Property** and associated revenue and market share losses

3rd Party Damages (to others)

Tangible (Physical) Damages
3rd Party Damages
(to others)

3rd Party Entities May Seek to Recover:
- Consequential Revenue Losses
- Restoration Expenses
- Legal Expenses
- Credit Monitoring Costs
- 3rd Party Entities may issue or be awarded civil fines and penalties

Available Insurance

Widely Available Cyber Insurance
- Subject to caveats on previous page (read your policy)

1st Party Damages
(to your organization)

Tangible (Physical) Damages

Financial Damages
Available Insurance

Excluded from traditional cyber insurance coverage

- Mechanical breakdown of your equipment
- Destruction or damage to your facilities or other property
- Environmental cleanup of your property
- Lost revenues from physical damage to your (or dependent) equipment or facilities (business interruption)
- Bodily injury to your employees

1st Party Damages
(to your organization)

3rd Party Damages
(to others)

Financial Damages
Property Insurance

Coverage under traditional property insurance is **uncertain**

- Many policies are silent (litigation risk)
- Some policies contain complete cyber exclusions (e.g., CL-380)
- Other policies contain potential exclusions
  - Electronic data
  - Terrorism
- Read your policy

---

- **Mechanical breakdown** of your equipment
- **Destruction or damage to your facilities** or other property
- **Environmental** cleanup of your property
- **Lost revenues** from physical damage to your (or dependent) equipment or facilities (business interruption)
- **Bodily injury** to your employees

---

**1st Party Damages**
(to your organization)

**3rd Party Damages**
(to others)

Financial Damages
New Cyber Insurance

New forms of Cyber Insurance are available to close gaps in property policies – affirming coverage

- Two insurers offer “gap-filler” coverage
- Another offers a standalone policy
- Challenge: lower limits are available than many property programs

Tangible (Physical) Damages

- Mechanical breakdown of your equipment
- Destruction or damage to your facilities or other property
- Environmental cleanup of your property
- Lost revenues from physical damage to your (or dependent) equipment or facilities (business interruption)
- Bodily injury to your employees

1st Party Damages (to your organization)

3rd Party Damages (to others)

Financial Damages
Available Insurance

“NEW” cyber coverage is available – mind the triggers

Questionable coverage in traditional casualty policies (similar to property policies)

Excluded from traditional cyber insurance coverage

1st Party Damages (to your organization)

Financial Damages

3rd Party Damages (to others)

Tangible (Physical) Damages

- **Mechanical breakdown** of others’ equipment
- **Destruction or damage to others’** or other property
- **Environmental cleanup** of others’ property
- **Bodily injury** to others

- **Financial Damages**
  - 1st Party Damages
  - Financial Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages

- **3rd Party Damages**
  - Tangible (Physical) Damages
Re-evaluate your “balance sheet”

Does your insurance cover the impacts you would suffer during an incident?
The only control that will actually pay for an incident:
- Forensics support within 24 hours
- Lost revenue

The only control that will provide “exculpability” to security managers and CISOs

One of the few controls that, once implemented, will get cheaper as your security posture improves

Cyber Insurance as an Incentive
Cyber Risk Reduction Curve

- Initial investments should be in cyber capability development—controls to protect and sustain
- As risk curve flattens, cyber insurance becomes an efficient means to further reduce risk
- Harmonizing the investment in technological and transfer controls requires better risk understanding

1. Technology Risk Reduction
2. Insurance Risk Reduction
What’s our cyber risk? Are we managing it?
Thank You!

Jason Christopher
Chief Technology Officer
jchristopher@axio.com | @jdchristopher | https://www.linkedin.com/in/jdchristopher
+ 1 929.575.5774
Additional Materials
CL380 Exclusion

Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means of inflicting harm of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

Clause 1.2 – Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme, or any other electronic system, in the launch and/or guidance system, and/or firing mechanism of any weapon or missile.