Building Success. Together.
Cyber Liability Risk Management: Insurance, Capital Markets and the Emergence of Comprehensive Security Standards

J. Kevin A. McKechnie
Executive Director, HSA Council
SVP, American Bankers Association
Major Health Insurer/Bank/Retailer Breaches
The per-record cost of a data breach varies widely by industry:

- Healthcare: $355
- Education: $246
- Financial: $221
- Services: $208
- Life science: $195
- Retail: $172
- Communications: $164
- Industrial: $156
- Energy: $148
- Technology: $145
- Hospitality: $139
- Consumer: $133
- Media: $131
- Transportation: $129
- Research: $112
- Public: $80

Healthcare and finance experienced larger costs.
Implications for Leading Network Equipment Manufacturer

- 400 new products a year
- 99% of all the products use Open Source
- 60% of all the code is Open Source

- 69% of all security defects are from Open Source (post release)
- Average defect age: 441 days
- 10% of high visibility vulnerabilities originate from open source
Code decay over time – router

- 289 new unique CVEs affecting the product during first 12 months of operations (approx 0.78 new CVEs per day during first 6 months)
- 48 new unique CVEs affecting the product 12 months before release
- Date of the oldest component found in the software (2009-01-13)
- 600% Increase In Unique Vulnerabilities Discovered In Last Year
- Released with total of 400 unique CVEs
- Released / compiled (2014-01-17)
- Product
- 689 unique CVEs as of 2015-01-26

Nov 2022. End of 100,000 hours average lifespan of LCD TV screen.

2012 Smart TV lineup launched: Nov/Dec 2011

Last firmware / SW update: Mar 2013 (*Approx. 178 unique CVEs affecting product at the moment of SW EoL)

Today. March 1, 2015. 584 unique CVEs in 23 components

One year product cycle

One year standard warranty for parts and labor from the date of purchase

7 more years of expected operation of the LCD TV (based on 100,000 hours average lifespan)

Approx. 0.58 new CVEs / day over the course of 23 months

Nov 2014: security update to patch curl, openssl, flash_player, ffmpeg, libpng and freetype

Estimated 2065 CVEs affecting Product by Nov 2022 based on historic 0.58 CWEs per day

(* date may not be fully accurate, as e.g. partial OTA updates may have been delivered after this date as well (see sec. update on Nov 2014))
Software ‘decays’ over time without patches

Software released circa Aug 2008. Total of 22 unique CVEs affecting total of 2 unique 3rd party components when the software was released. None of these had CVSS score of 10.

Same software in Feb 2015. Total of 582 unique CVEs affecting total of 60 unique 3rd party components. 74 of these had CVSS score of 10.

Challenge: Many products are delivered with unpatched, known vulnerabilities
Software Composition Analysis is Needed Because Code Travels …

- Free Open Source Software (FOSS) under GPL, AGPL, MPL, Apache and other licenses
- Commercial off the shelf (COTS) 3rd party code
- Outsourced code development
- Copy-paste code
- First party code
- Floodgate – Software Signoff
- Sea of downstream businesses that use software from upstream

Outdated, vulnerable code
Unauthorized, potentially malicious and counterfeit code

© 2016 Synopsys, Inc.
The Cyber Market – Scale Metrics

• There are about 60 markets in the U.S., U.K., and Bermuda with about 130 individual underwriters.
• The Top 15 underwriters held 83% of the market in 2016.
• Fitch and A.M. Best estimate $1.35 Billion direct written premium in 2016, up 35% over 2015.
• The Betterley Report estimates about $3.5 Billion in 2016.
• Loss ratios are improving 46.9% in 2016 down from 51.4% in 2015.
2016 Cyber Insurance Buying Guide

Why buy Cyber Liability protection?

How much coverage and what kind of coverage to buy?

What perils can Cyber Insurance cover?

Risk mitigation: the UL CAP 2900 Standard vs. Everything Else
Executive Summary

Why We Need Cyber Insurance

As cyber risks grow, senior management and boards of directors are increasingly focused on enterprise cyber solutions that includes risk mitigation, risk transfer and response/recovery.

Problem:

Until recently, no accredited comprehensive cyber risk strategy existed to help enterprises manage cyber risk. Accordingly, organizations are clamoring to transfer cyber risks through the purchase of insurance products until their own risk management systems can be upgraded. Most organizations are unaware of or intimidated by cyber insurance products precisely because they are unaware of the gaps in their cyber security strategy.

Solution:

The FSSCC Cyber Insurance Task Force developed a Purchasers’ Guide to Cyber Insurance earlier this year, to guide those considering the purchase of cyber insurance. It identifies key questions a prospective policyholder should ask when considering the purchase of cyber insurance and includes an appendix for sophisticated purchasers who want to control the quality of software products they buy.
What does a Cyber Liability Claim Look Like?

2015 Average Claim Payout = $4.8 Million Large Company; $1.3 Million Healthcare Sector; $673,767 for all claims
2016 Average Claim Payout = $3.04 Million Large Company; $726 K Healthcare Sector; $495 K for all claims

Average No. of Records lost = 2015/3.2 Million; 2016/2.04 Million

2015 Average Cost of Crisis Services = $499,710 (largest claim component)
2016 Average Cost of Crisis Services = $357,000 (largest claim component)

Average Cost of Legal Defense = $434,354 – 2016 - $130K
Average Cost of Legal Settlement = $880,839 – 2016 - $815 K

2015 Targets: Healthcare Sector breached most = 21%; Financial Services 17%
2016 Targets: Healthcare Sector breached most = 19%; Financial Services 10%

2015 Top Data Exposures = PII (45%), PCI (27%), PHI (14%)
2016 Top Data Exposures = PII (40%), PCI (27%), PHI (15%)

2015 Breach Cause? Hackers (31%) Malware/Virus (14%) Mistakes and espionage (11%)
2016 Breach Cause? Hackers (23%) Malware/Virus (21%) Mistakes and espionage (16%)

Source: NetDiligence 2015/2016 Cyber Claims Study
What does a Cyber Liability Claim Look Like?

2015 Claim Expenses by Major Category

- Crisis Services: 78%
- Legal Defense: 8%
- Legal Settlement: 9%
- Regulatory Defense: 1%
- Regulatory Fines: 1%
- PCI Fines: 1%

1%
What does a Cyber Liability Claim Look Like?

2016 Claim Expenses by Major Category

- Crisis Services: 75%
- Legal Defense: 3%
- Legal Settlement: 9%
- Regulatory Defense: 8%
- Regulatory Fines: 0%
- PCI Fines: 5%

American Bankers Association
Reasons to Consider Cyber Insurance

1. Insurance places **a dollar value on an organization’s cyber risk**.

2. The underwriting process can help organization’s **identify cybersecurity gaps and opportunities for improvement**.
   a) In the same way property insurance has helped create safer buildings, cyber insurance can promote safer cybersecurity practices and policies.

3. In addition to providing the traditional risk transfer function, many cyber insurance policies **bring supplemental value through the inclusion of risk mitigation tools**.

4. Regulators may also focus increasingly on cyber insurance as a **key facet of a regulated entity’s operational resilience**.
   a) The SEC has issued guidance noting that cybersecurity risk disclosures must adequately describe the nature of the material risks and include a “description of the relevant insurance coverage.”

**TIP:** Only buy coverage you need; Liability towers use “off-the-shelf” insurance policy forms; discuss customizing a product that covers your company’s risks in order to avoid paying for unnecessary coverage.
Cyber Insurance Coverage

Cyber insurance can cover your own costs/expenses (first party coverage) or amounts you are liable to pay others (third party coverage):

**First Party Coverage** (costs to YOU):
- Crises Management & Identity Theft Response – client notification and forensic investigation costs
- Cyber Extortion costs
- Network/Business Interruption
- Regulatory fines/penalties

**Third Party Coverage** (what you owe OTHERS):
- Privacy Liability – claims from clients/customers for failing to protect personal or confidential information.
- Network Security Liability – claims from transmission of malware/viruses
- Media Liability - likely only available for online content or activities
Decisions to be Made

**Whether or not to purchase**

- Depends on what kind of information the organization has (i.e. credit card numbers and passwords, health records, trade secrets, patents, etc.) and
- Potential ramifications if this information is compromised or exposed (reputational damage, regulatory actions, litigation, operational impact).

**How much to buy**

- While there is some regulatory guidance, much of the determination is dependent upon an organization’s risk appetite.
- The top ten U.S. banks purchase up to $400 M+ of cyber insurance.

**What coverage to buy**

- It is important that purchasers obtain coverage for both types of loss - first party coverage (crisis management and identity theft response, cyber extortion, data asset protection, network business interruption) and third party coverage (network security liability, privacy liability).
Organizations’ cyber maturity greatly effects the amount of coverage available and the terms and cost of the coverage. Companies can do a lot to shore up their information security policies and practices to increase the availability of coverage and reduce the cost of coverage.

Categories of Information Insurers need to Underwrite Cyber Insurance:

- Dedicated Information Security Resources
- Information Security Policies and Procedures
- Employee Training and Education
- Incident Response Planning
- Security Measures
- Vendor Management
- Board Level Approval or Oversight of the IS Program
The US government has publicly released two tools that are useful for businesses assessing cyber risks and identify steps to meet those risks.

- In 2014, the NIST released the **Framework for Improving Critical Infrastructure Cybersecurity**, which is a voluntary framework, based on existing standards, guidelines and practices, to help reduce cyber risks.

- In 2015, the FFIEC released its **Cybersecurity Assessment Tool**. This tool is intended to help institutions identify their risks and determine their cybersecurity preparedness in a repeatable, measurable way. It allows an organization to analyze its Inherent Risk Profile and its Cybersecurity.

TIP: If your company increases its cyber maturity through application of the NIST/FFIEC frameworks or by analysis using 3rd party tools (Reprivata/Synopsys/UL 2900), request re-underwriting to reduce your premiums.
UL Cybersecurity Assurance Program (UL CAP) will be *Product Oriented & Industry Specific* with these goals:

- Reduce software vulnerabilities
- Reduce weaknesses, minimize exploitation
- Address known malware
- Increase security awareness

**Product service offerings apply to:**

- Connectable Products
- Products Eco-Systems
- Products System Integration
- Critical IT Infrastructure Integration

---

**UL 2900-3:** Organizational Process

**UL 2900-2-1, -2-2:** Industry Specific Requirements

**UL 2900-1:** CAP General Requirements/
UL Cybersecurity Assurance Program

Leverages use of tools in the Synopsys Software Integrity Platform

- Cybersecurity Assurance Program (CAP) in includes:
  - **Malformed Input Testing** (Fuzz Testing and DoS Testing)
    - For all externally accessible protocols
    - Also addresses application level protocols
  - **Software Composition Analysis**
    - Compiled code
    - Up to 90% of all code is third-party
  - **Malware Analysis**
    - Know malware
  - **Static Code Analysis** – Source Code
  - **Runtime Analysis** – Running code
  - **Penetration Testing** – Hands on testing
UL Cybersecurity Assurance Program

Underwriters Labs CAP 2900 series –

- Addresses known vulnerabilities at the time of certification (i.e. CVEs catalogued in the NVD)
- Performs baseline weakness assessment for potential “zero day” vulnerabilities (CWSS and scoring priorities from others’ Top ‘N’ lists)
- Addresses known malware at time of certification

Addressing the most relevant CWEs, establishes a baseline to mitigate weaknesses that, if otherwise exploited, could be vectors of attack; becoming zero-day vulnerabilities
Currently, Reprivata is the only company to secure the UL 2900 CAP certification and the only software to pass all of the testing regimes Synopsys established for the UL test.

Community of Trust Private Network – establishes contractual relationships between electronic counterparties which define and limit liabilities, require all members to carry cyber liability insurance and to maintain CSF Tier 3 Cyber Maturity (Like Sarbanes Oxley for Cyber Risk Disclosure)

Reprivata Encrypted Core Software/Hardware – a secure platform that surrounds an organization’s existing software/hardware infrastructure allowing secure communications, application development, and counterparty identification.
Structured Protection Instruments (SPIs)

Not an insurance product – Catastrophic Cyber Event Protection Contract
Pays a set financial benefit based on known contractual elements
Pays as soon as those elements are triggered, not once claim is adjudicated
Declared Cyber Event – Material Change in Stock Price Disclosure
Strike Provision Trigger – Payment for share price decline > 10% > 20% > 30%
Backed by “A rated” syndication of financial institutions
Financial benefit size of up to $1 Billion

May have regulatory capital relief for bank holding companies under BASEL III

Illustration of quarterly coverage:
- Cost $4.5M
- Declared cyber event
- Stock declines 20%+, benefit = $225,000,000 (50 to 1)
- Stock declines 30%+, benefit = $500,000,000 (111 to 1)
Proposed cyber rules are increasingly focusing on enterprise-wide management, applies to enterprises $50B+ in combined operations.

It’s like HIPAA and Sarbanes/Oxley for Cyber:

- Each organization that is a “covered entity” must compel organizations with which it does business or is affiliated to adhere to the same cyber maturity structure applicable to the parent – just like HIPAA for health insurers.
- Each “covered entity” must require a “Chief Risk Officer” to report on the organization’s cyber posture to the Board of Directors – just like SOX requirements for public companies.
The proposed Cyber rule contains 5 broad categories of cyber enterprise risk management:

1. cyber risk governance;
2. cyber risk management;
3. internal dependency management;
4. external dependency management; and,
5. Incident response, cyber resilience and situational awareness.

Would apply to 3rd parties doing business with a covered entity

Covered entities would also be required to define internal and external cyber risks and develop resiliency plans to ensure continued operation of critical business functions during a cyber incident.
Know How The Policy Works: Key Triggers & Events

When is coverage triggered?

• A policy requiring a “Claim” to be made before coverage applies may not be in line with the expectations of the insured. Rather, a policy that is triggered upon the “discovery” of a data breach may be more appropriate to cyber risks.

When is notice to the insurers required?

• If a policy is not structured properly, there could be no opportunity to provide the carrier “notice” of a Claim before significant costs are incurred.

How are breach counsel and vendors selected?

• It is prudent to select these vendors in advance of a breach and get any contractual and conflict measures resolved with these vendors prior to a breach.
• Make sure your insurance provider approves of the use of the vendors (*Note: many insurers have prequalified breach response specialists available to assist clients with responding to data breaches).

TIP: Include key notification requirements in the incident response plan and pinpoint a key stakeholder to make sure those notification obligations are appropriately satisfied.
Portable electronic device exclusion
If the device leading to a cyber breach is portable, many policies could exclude coverage completely for any resulting loss – “Edge Devices”

Intentional Acts Exclusion
Most cyber insurance policies do not adequately provide for both first party and third party loss.

Nation/State, Terrorism, Cyber Terrorism Exclusions/Acts of God Clauses
This can result in coverage being precluded simply based on who or what caused the breach – Coverage against certain bad actors needs to be proved in forensics
Negligent Computer Security Exclusion
Some policies exclude coverage if data is unencrypted or if the Insured has failed to appropriately install software updates or security patches.

Sub-limits
Many policies also have sublimits that may apply for things like breach notification costs, forensic expenses, credit monitoring costs, business or network interruption.

Vicarious Liability/Vendors
Many standard Cyber policies exclude coverage for data an organization has entrusted to a third-party vendor who is breached.

TIP: Request removal of the exclusion from the policy. If insurer will not remove, request an exception to the exclusion, to cover losses involving portable devices if the data is encrypted.
Takeaways

In addition to the “tips” provided, below are some of the best practices firms should consider while purchasing cyber liability insurance:

• Take a proactive approach by taking the time to examine your networks, cybersecurity practices, training your employees, maintaining rigorous self and vendor testing, and promptly remediating issues.

• Carefully review the terms of your policy. If you do not understand what something means, that often means it is not clear and could lead to coverage denial or litigation.

• Look closely at how the policy is constructed, especially the insuring agreement to ensure coverage is triggered upon the discovery of the breach, not after a claim.

• Include key notification requirements in the incident response plan and pinpoint a key stakeholder to make sure those notification obligations are appropriately satisfied – then, PRACTICE YOUR PLAN!
Takeaways

• Include selected breach counsel and vendors (forensics firm, public relations, crisis management firms) in the incident response plan.

• Discuss your selected breach vendors with the insurers prior to policy purchase to ensure they will approve the use of those vendors if there is an incident.

• Remember to include a step in your incident response plan to notify the insurers of the use of the vendors after a breach.

• Request removal of sublimits from policy. If sublimits cannot be removed, negotiate highest sublimit possible for least associated cost.

• Examine the services offered and negotiate coverage for services the Insurer may offer.

• Ensure all third party vendors with whom business is conducted maintain Cyber insurance policies of their own – Reprivata System does this automatically.

• Review “acts of God” exclusions carefully in Cyber policy, negotiate to limit exclusions as much as possible.
What Should NCSL Do Next?

- Petition the Department of Homeland Security for security clearances in order to participate with federal law enforcement officials in threat discussions.

- Use the appropriations process in your state to:
  - Demand software vendors sell products with no known vulnerabilities
  - Encourage state agencies to become a Community of Trust (CoT)
  - Encourage states CIOs/CSOs to adopt the UL 2900 CAP certification
  - Purchase Cyber liability insurance or SPI products to safeguard state treasury
  - Hold software and hardware companies liable through contract language
Contact

Kevin McKechnie
Executive Director, ABA HSA Council

Kmckechn@aba.com

202 663 5172 O
202 320 3360 C

American Bankers Association
1120 Connecticut Avenue NW
Washington, DC 20036