Who holds your cyber keys?

14 JANUARY 2021

Milliman

Panelists

Thomas A. Ciano
Senior Vice President, Practice Leader, Executive & Professional Risk Solutions
USI Insurance Services

Chris Harner
Managing Director, Cyber Risk Solutions
Milliman

Aaron K. Tantleff
Partner
Foley & Lardner LLP, Technology Transactions & Outsourcing and Privacy, Security & Information Management

Milliman

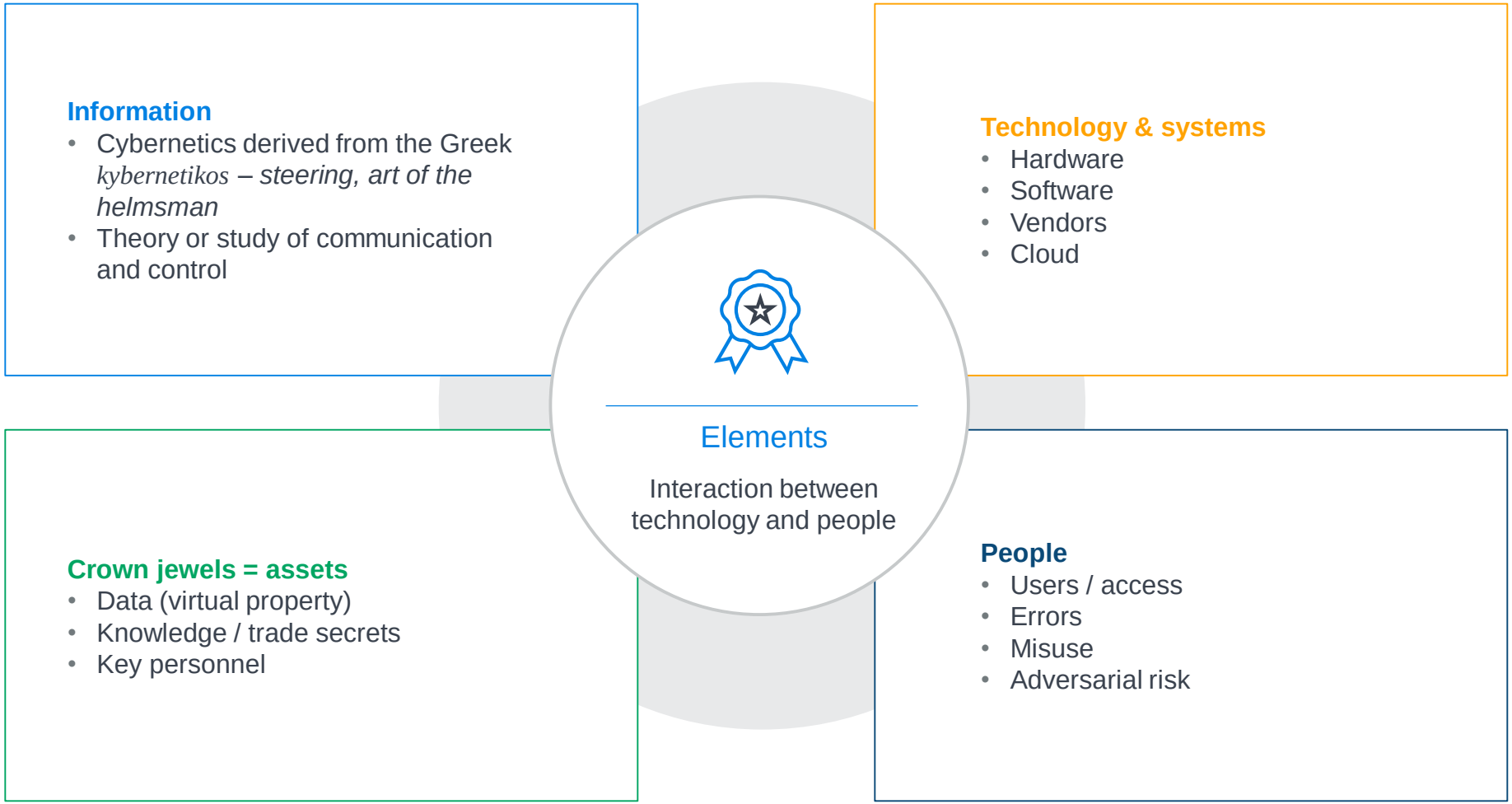
Who holds your cyber keys?

Chris Harner

JANUARY 14TH, 2021

The problem

Cyber is not just a technology problem, it is also a people problem



Cyber risk principles

Cyber risk requires a strategy based on effective assessment and planning

Holistic mapping

- Cyber is the ultimate enterprise risk: it involves IT, Risk, vendors, business processes, assets, geography, legal and compliance, etc.
- Go beyond 1st order thinking, i.e., obvious parts and relationships. Mapping must capture 2nd and 3rd order phenomena
- Understand and rationalize complexity

Identify critical relationships

- Mapping should diagnose linear and nonlinear relationships:
  - Dependencies
  - "Blind spots" and bottlenecks
  - Vendors
  - Assets
  - People
  - Controls

Prioritization

- Data driven modeling
- Apply critical lenses:
  - CIA triad
  - Trade-offs
  - "Known Unknowns"
- Validate goals
- Define next steps

Cyber Risk Strategy

Key issues in cyber

Constant breaches highlight the following repeat and emerging issues

Normalcy bias

Underestimating the frequency and severity of risk events is endemic. Playbooks assume systems will perform under duress like during BAU.

Propagation velocity

Breaches often occur from unanticipated end point. Dwell time can drive the severity of a breach.

Cascading failure

Risks are typically evaluated in a siloed, linear fashion instead of an interconnected system. Nonlinear relationships are rarely if ever measured.

Recovery serendipity

Recovery of assets and the speed of recovery are critical to understanding the impact.

Attack attribution

It is difficult to forensically prove attribution of an attack. It is unclear whether courts will take governments' attribution statements at face-value.

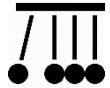
Insurance coverage

Some insurers may add policy language to exclude acts of war to mitigate exposure. However, it is unclear if the war exclusion is enforceable.

War exclusion

Legal definitions of traditional kinetic war is vague.

Cyber war is non-kinetic while it is difficult to prove attribution.



Law of unintended consequences

The impact of a cyber breach results in 2nd and 3rd order effects throughout the company and its supply chain.

Cyber Liability

Transfer of Risk Through Insurance

Traditional Property and Casualty Policies

- Provide protection for bodily injury and property damage from physical perils

Fidelity or Crime Policy

- Provides protection against the theft of money, securities and tangible property

Cyber Liability Policy

- Provides protection for network security, privacy and the theft or release of confidential information – both personal and business

Property & Casualty Insurance

Not developed to cover cyber exposures

- Language did not specifically address the exposures
- Pricing did not contemplate the risk
- Early avenues of possible coverage have been closed

Emerging expansion of cover under property policies

- Some expansion to address business interruption

Fidelity or Crime Insurance

Typically Includes

- Computer Fraud
- Funds Transfer Fraud
- Forgery

Often inadequate to address today's exposures

- Nuances in policy language and varying interpretations leave gaps in coverage

Look to add affirmative coverage

- Social Engineering – Fraudulent Transfer Coverage

Cyber Liability Insurance

Addresses Network Security and Privacy Liability Incidents

- First Party Costs – the costs an organization faces when dealing with a breach incident
- Third Party Liability – the costs an organization faces for their liability to others as a result of a breach incident

First Party Costs

Typical Breach Event Costs Include

- Legal guidance
- Forensics investigation
- Crisis management / public relations
- Breach notification costs
- Credit monitoring

Other Business Costs Include

- Business interruption/system failure (dependent?)
- Data restoration
- Extortion (ransomware)
- Cyber crime – social engineering
- Consequential reputational loss

Third Party Costs

Civil Lawsuits

- Consumer class action
- Corporate or financial institution suits
- Credit card brands
- PCI fines, penalties and assessments

Regulatory Actions

- State AG investigations
- FTC investigations
- Health and human services – i.e. HIPAA
- Foreign privacy entities – GDPR

Access to Key Resources

At the time of loss

- Forensics firm – who, what, where, when
- Attorney for various state compliance requirements
  - Including contractual indemnification obligations
- Public Relations expense – brand protection
- Credit monitoring, notification assistance
- ID restoration services
- Licensed investigator/fraud specialist

Pre-breach loss mitigation services

- Access to free and discounted services

Insurance as a Last Line of Defense

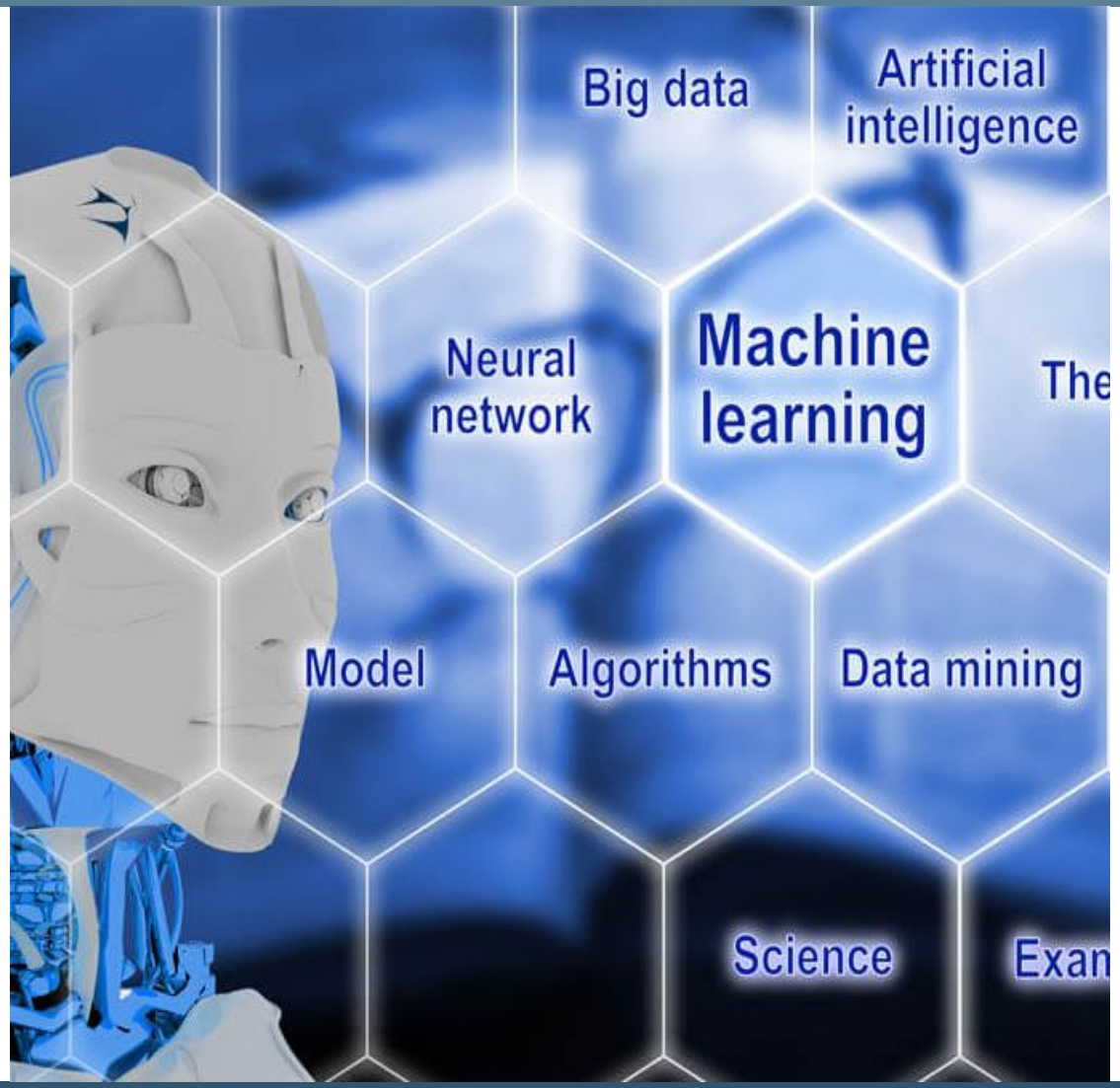
IT security, policies and procedures don't always work!

- Cyber insurance fills gaps in "traditional" insurance
- Acts as a financial backstop to the organization
- Assists the organization with continuity planning
- Helps to establish relationships with key vendors
- Demonstrates an organizational commitment to network security and privacy

FOLEY

FOLEY & LARDNER LLP

Legal & Insurance Considerations



Liability and Litigation

- Secretary of Education authorized to take *appropriate actions* for violations of FERPA, such measures have included:
  - Family Policy Compliance Office (FCPO) Investigations
  - Cease and desist orders
  - Termination of eligibility to receive federal funding (albeit this remedy has yet to be used by DOE)
  - Third party service providers may be banned from receiving PII for up to five (5) years
  - No criminal provisions or private right of action
- Reputational costs
- Recent litigation
  - March 30, 2020, FCPO webinar guidance: video recordings of virtual classroom lessons may be an “education record” if they directly relate to a student and are maintained by or on behalf of an educational institution AND non-disclosure provisions may still apply if the recording contains PII from student education records.
  - 2018, Agora Charter School violated FERPA by requiring parents to accept a third party’s terms of use that were not FERPA compliant (resulting in a forced waiver of FERPA rights)
  - 2017 Wachter Letter, access to education records involving multiple students requires segregation/de-identification of other students unless it destroys the meaning of the record

Regulatory Expectations

FERPA requires	PPRA restrictions	Additional state law requirements

• Individual rights to access, correct, and consent to the disclosure of PII
• Annual notification of rights
• reasonable methods to ensure the security of PII
  • Implement and maintain a comprehensive data security program, including remote work access controls
  • Incorporate FERPA requirements into service provider contracts, provided the school official exemption is met.
	• Restricting the administration of surveys, analyses, evaluations, or psychological exams covering sensitive categories of information
	• Restricting the collection and use of PII for marketing purposes
	  • Does not include collection for the purpose of developing, evaluating, or providing educational products or services
		• Several states, including California (SOPIPA) and Massachusetts, have enacted laws setting security requirements for PII
		• State breach notification statutes
		• State privacy laws (e.g. CCPA, where an institution is for-profit)
		• State open records laws

Which Policies Cover Cyber?

Traditional commercial general liability and property insurance policies typically exclude cyber risks from their terms

May or may not cover third party damages

Network/Information Security and Privacy Liability Coverage

- Generally covers expenses **directly** incurred as a result of a cyber incident, e.g., legal expenses, cyber extortion, forensics, data restoration, public relations, notification, credit monitoring and identity restoration costs
- Watch out for exclusions
- May also include administrative and regulatory proceedings, fines, and penalties

Business Interruption Coverage

- Generally covers **indirect** losses, e.g., lost profits, fixed expenses and extra costs incurred during the failure

Media Liability Coverage

- claims for losses caused by intellectual property infringement (excluding patent infringement) resulting from an insured's advertising (print and online)

Technology Errors and Omissions Coverage

- Coverage for error in performance and failure to perform services
- Directed towards service providers offering technology service and products
- Covers negligence and breach of contract claims

What is “silent cyber”?

- Cyber events not defined in traditional coverage but where a court has decided that a claim is covered
- Courts have found traditional business insurance policies may cover certain cyber incidents
  - Uncertain recovery
  - Long, slow process
  - Expensive recovery
- Stand-alone cyber insurance
  - Less ambiguity
  - Avoids disputes
  - Quicker recovery