Technology’s Dark Side: New Threats to the Practice of Architecture

TH104

Thursday, June 21, 2018, 7:00AM -8:00AM

1 HSW

This presentation is protected by U.S. and international copyright laws.

Reproduction, distribution, display and use of the presentation without written permission of the speaker is prohibited.

This program is registered with the AIA/CES for continuing professional education. As such, it does not include content that may be deemed or construed to constitute approval, sponsorship or endorsement by AIA of any method, product, service, enterprise or organization.

The statements expressed by speakers, panelists, and other participants reflect their own views and do not necessarily reflect the views or positions of The American Institute of Architects, or of AIA components, or those of their respective officers, directors, members, employees, or other organizations, groups or individuals associated with them.

Questions related to specific products and services may be addressed at the conclusion of this presentation.

Speakers List

Frank Musica, Assoc. AIA, Esq.

Risk Management -- Senior Specialist

Victor O. Schinnerer & Company, Inc.

Learning Objectives

- Realize the exposure to public safety through unintended violations of information security requirements.
- Understand the scope of damages caused by the breach of the architect's professional or contractual duty to keep client information confidential.
- Recognize the endangerment of projects and firm operations because of damage to or ransoming of firm information by cyber criminals.
- Evaluate the harm caused by the invasion of the privacy through the improper use of photography, remote sensing, and drones.

Surviving the Transition

Three Basic Precepts of the Evolving Practice Environment

Surviving the Transition

Three Basic Precepts of the Evolving Practice Environment

Surviving the Transition

Firms are evolving from providing the basic design of capital assets into sources of intellectual property that is shared throughout the planning, creation, and operation of the built environment.

Surviving the Transition

New technologies both aid and force the transition from a profession based on learned and licensed professionals to one based on the creation and secure transmission of digital information.

Surviving the Transition

Firms must recognize the moral, legal, and financial implications of their use of technological enhancements to their services.

Today's Program:

- Information Security
- Confidentiality
- Personal Injury Exposure
- Cybercrime and Cyberliabilty

Information Security

Information Security

The Opportunity and the Threat

BIM and other programs enable design firms to work more closely with stakeholders in their projects.

Digital deliverables:

- Provide the opportunity to exchange information easily.
- Reduce errors in design and communication.
- Create the peril of inappropriate information use.

Information Security

Firms must realize the risk to the client or to the public through violations of information security requirements.

Federal Contract (FAR) Requirements:

- Safeguarding Covered Defense Information (CDI)
  - Unclassified controlled technical information
  - Other information that requires dissemination controls
- Basic Safeguarding of Covered Contractor Information Systems

Information Security

Other Federal Requirements:

- Department of Homeland Security (January 2017)
- General Services Administration (January 2018)

If you have a government contract with another federal executive agency, it will be subject to the cybersecurity requirements in the FAR Basic Safeguarding of Covered Contractor Information Systems. It requires 15 safeguarding controls.

Information Security

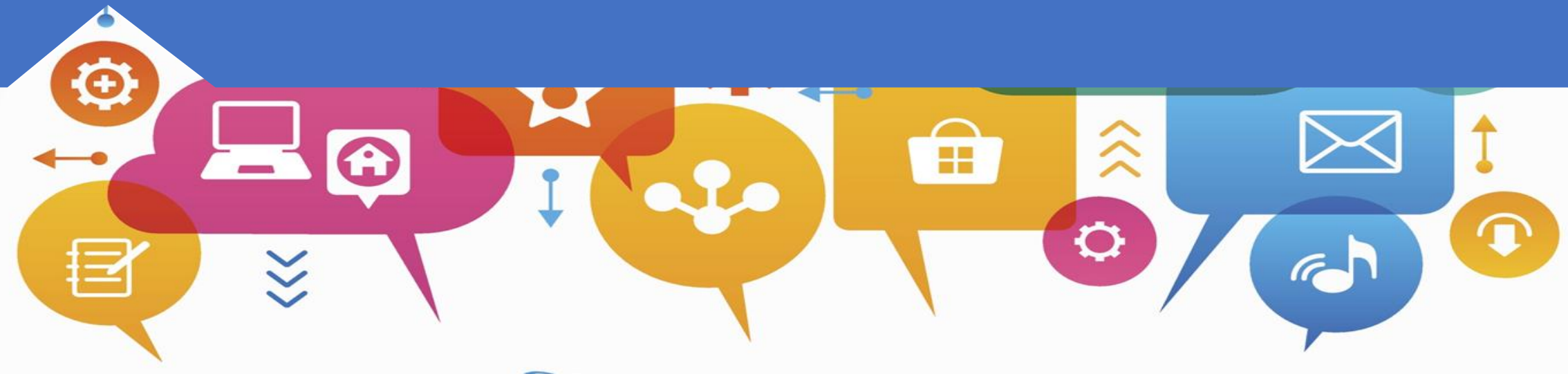
National Institute of Standards and Technology Guidance:

Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*

Federal requirements for Covered Defense Information include:

- Assessment of Security Measures
- System Security Plan
- Plan of Action and Milestones

Confidentiality



Confidentiality and Liability

Business exposures

- Violation of confidentiality and non-disclosure agreements
- Willful exposure of client information
- Compromised security of infrastructure or building through publication, inadvertent disclosure, or hacking
- Inadequate protection of internal firm trade secrets, personally identifiable information, or financial controls

Confidentiality and Liability

Professional liability exposures

- Disclosure of confidential information during the negligent performance of professional services by the firm or its subconsultants
- Jeopardizing security through negligent responses to threats identified by client or regulations
- Failure to meet the standard of care for recognizing cyber security violations that change design parameters or design results

Personal Injury Exposure

Personal Injury Exposure

Use of remote sensing devices can expose firms to:

- Professional liability claims
- Property damage claims
- Bodily injury claims
- Personal injury claims

  Personal injury liability insurance is designed to protect the policy holder from lawsuits filed because of alleged damage to an individual resulting from invasion of privacy.

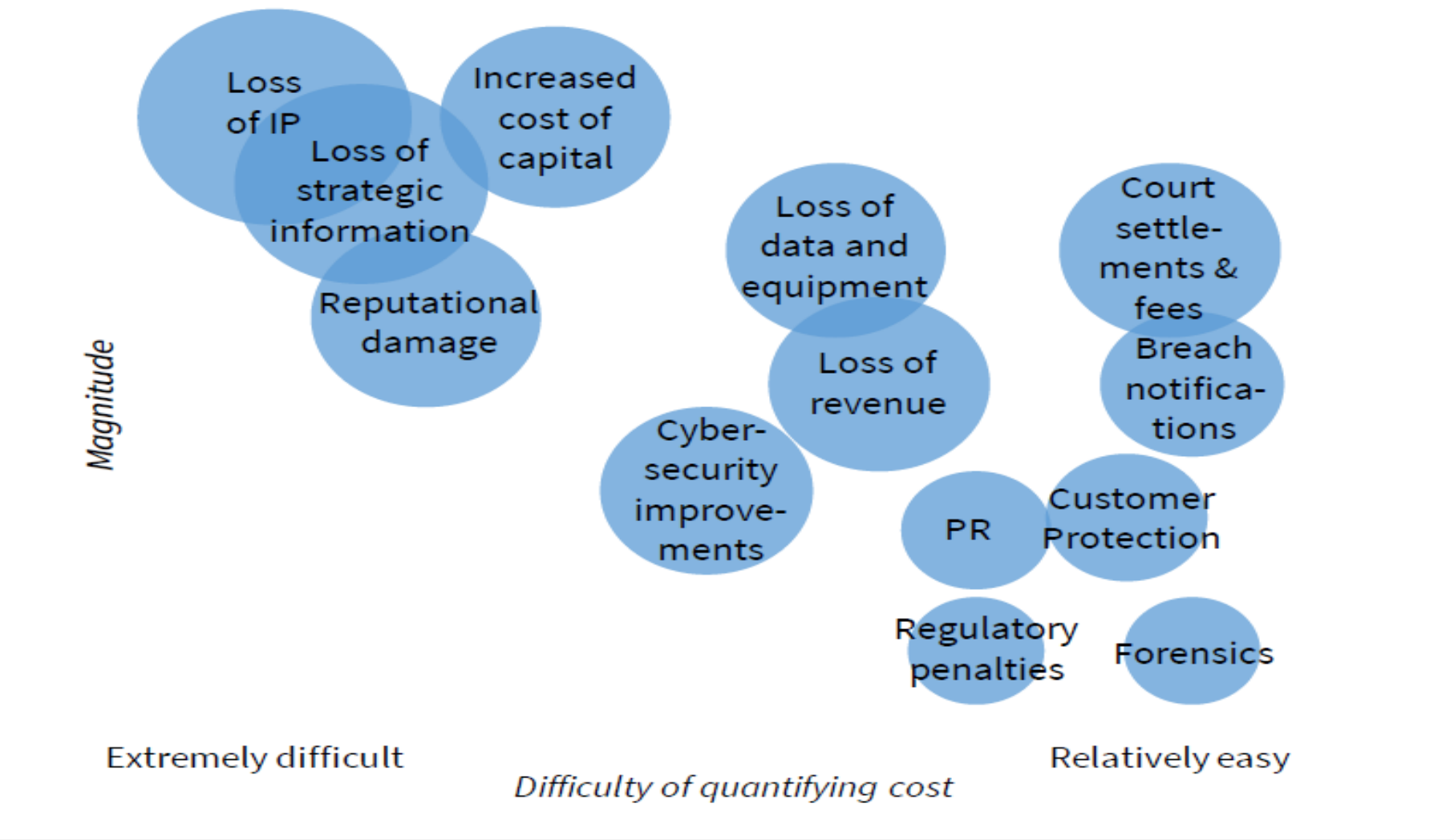
Personal Injury Exposure

Use of remote sensing devices means you must have:

- Professional Liability insurance coverage
- Commercial General Liability insurance coverage
- Aircraft Liability coverage or a CGL endorsement
- Cyberliabilty coverage

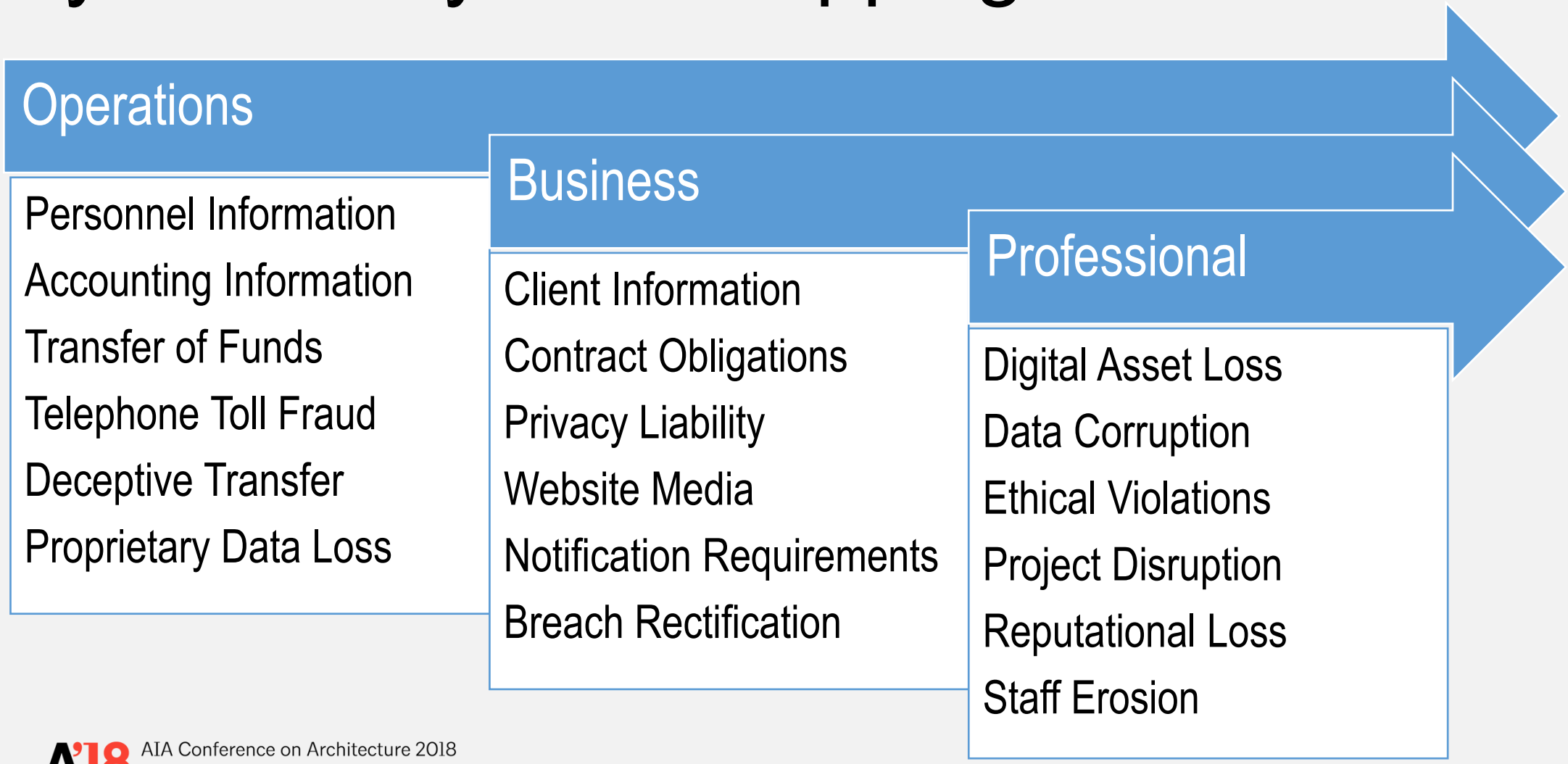
Cybercrime and Cyberliabilty

Cost Components of an Adverse Cyber Event



Council of Economic Advisors ***The Cost of Malicious Cyber Activity to the U.S. Economy***, February 2018

Cyberliability Risk Mapping



Cybercrime

1. As technology and digital connectivity evolve, companies face menacing new threats.
2. Every day – even as cybersecurity improves – the exposure increases.
3. It's a vicious cycle. As technology advances, our risk for new, sophisticated attacks increases.

Can your company withstand a significant cyber attack and continue operations?

Cyberliability

Identify your most critical assets

What do you have that is most valuable to others?

Gather intelligence on cyber threats

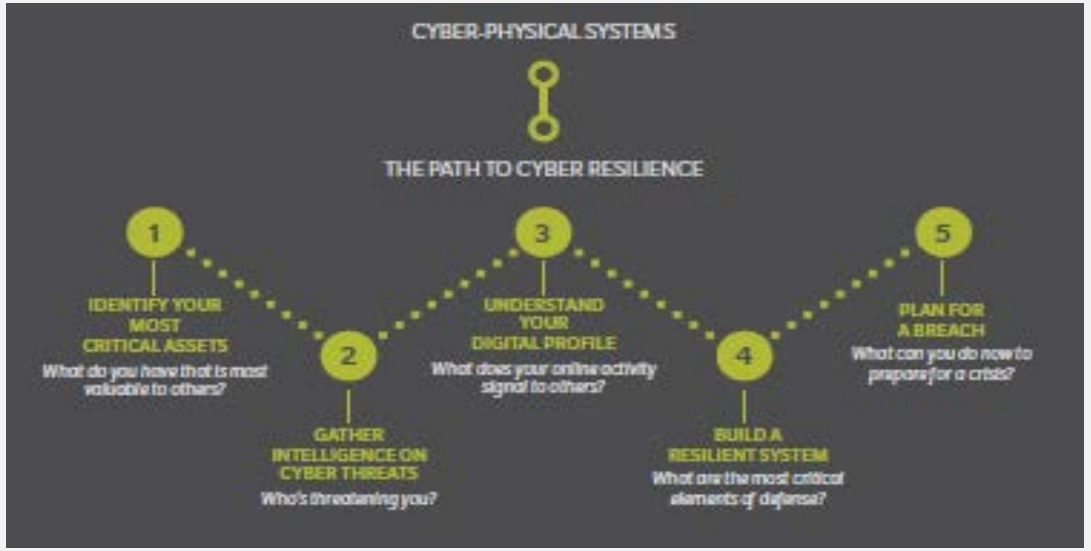
Who's threatening you?

Understand your digital profile

What does your online activity signal to others?

Build a resilient system

What are the most critical elements of defense?



Plan for a breach

What can you do now to prepare for a crisis?

Cyberliability

A comprehensive risk management program that focuses on internal and external threats to information and the systems and people maintaining the information is a critical element in enterprise risk management:

- Take steps to secure systems, guard digital assets, protect confidential information, and maintain productivity
- Limit employee access to confidential and sensitive information, such as intellectual property, digital design data, and private information about clients, employees, and business partners
- Educate employees on the dangers of digital data security and the need to follow proper procedures

Cyberliability

Common sources of cyberliability:

- Insiders who are dissatisfied or recognize their ability to use that access for harm or personal profit.
- Past employees who either take digital assets with them or corrupt firm systems and information to inflict revenge.
- Intruders who seek to steal personally identifiable information for financial gain.
- Hackers who know that confidential project data is vulnerable and hold digital information hostage until a ransom is paid.

Cyberliability

The National Institute of Standards in Technology (NIST) has published a cyber security framework that attempts to define standardized cyber security activities, desired outcomes, and applicable references that constitute sound cyber security.

It is organized under five continuous functions:

Cyberliability

- **Identify** – Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement appropriate activities to identify a cyber security event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cyber security event.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and restore capabilities or services impaired due to a cyber security event.

Cyberliability: Insurance Coverage Needs

- Breach rectification including digital property replacement coverage
  - Business interruption and digital asset loss
  - Replacement, restoration, or reconstitution of digital property
- Breach liability, including website media coverage
  - Privacy liability, regulatory actions, website liability
  - Intellectual property infringement and personal or advertising injury
- Digital crime
  - Cyber extortion
  - Deceptive transfer of funds
- Cyber Breach Response Team assistance

Contact Information

Frank Musica, Assoc. AIA, Esq.

Risk Management -- Senior Specialist

Victor O. Schinnerer & Company, Inc.

frank.d.musica@schinnerer.com

The Schinnerer Risk Management Website Information and Educational Courses are at:

www.Schinnerer.com/SchoolofRiskManagement

Thank you!