Cybersecurity, commercial enterprise and national security

Managing technology and risk to drive prosperity and economic growth

Jeremy Straub

North Dakota State University

Computing as an ‘everything’ enabler

- Computing and information technology systems are integral to most aspects of modern-day humans’ everyday lives.
  - They control water, power, gas and other essential services.
  - They are used by most individuals as part of their employment.
  - They provide entertainment.
- Because of this, human prosperity and the success of businesses and society in general is tied to these systems operating correctly.

Cybersecurity as a risk to ‘everything’

- Cybersecurity vulnerabilities present a risk to these operations and, via this, to society.
  - Disabling / denying access to key systems
  - Disabling / interfering with key systems at times of key need
  - Maloperation of systems
  - Data capture and exfiltration
  - Ransomware
  - Many other examples

This presentation

- This presentation discusses the risk management calculus of cyber threats to society, broadly, and its components: private enterprise, government, individuals and academia.
- A framework for discussing cyber threats in a broader-than-affected-system-operator context is presented.

What is risk management?

- Identifying risks
  - You can’t specifically prepare for things you haven’t identified
  - General response preparations and cyber hygiene can be helpful across the board
- Assessing risks
  - How bad would the issue be, if it occurred?
  - How likely is it to occur?
- Preparing for risks
  - Mitigation of risk occurrence
  - Preparation for response

What is risk management?

- Key areas of risk management
  - Understanding the enterprise
    - Data
    - Processes – electronic and business
    - Other factors – e.g., employee considerations (morale, co-response issues, etc.)
    - Understanding importance and impact of systems and data to operations and the importance of operations to the enterprise
  - Understanding risks
    - Frank identification of areas of risk / vulnerability
    - Accurate assessment of likelihood
    - Accurate assessment of impact

Risk calculus

- Risk equation:
  - Likelihood of occurring x impact of occurrence

- Can be used to assess overall risk posture (summing)
- Can be used to rank risks for prioritization (sorting)

- Highly reliant on the accuracy of the underlying data
- Potentially subject to systematic issues / bias

Beyond enterprise risk

- Many enterprises have impact of risk occurrence beyond the costs to the enterprise itself
- A municipal power facility, for example, may have limited liability for an outage caused by a cyber attack
  - May interfere with numerous businesses
  - May interfere with individuals' daily lives
  - May deny critical services
    - Hospital equipment
    - Heat in winter
    - Air conditioning in summer for vulnerable populations

Beyond enterprise risk

- Enterprises must consider impact beyond the entity in designing appropriate risk management plans

- An example: a small business realizes that it cannot get enough insurance to cover a large-scale breach
  - It identifies the impact of the breach being the caseation of its operations
  - It may not develop a response plan for this worst-case scenario (beyond shutdown)
  - This may drive additional focus on risk mitigation

Assumption of response aid

- Many enterprises assume that they will be able to get help in response
  - Federal agencies – FBI, NSA, DHS, etc.
  - State / local assistance
  - Insurance company-provided
  - Hire on-demand
- This may not be a valid assumption
  - Agencies prioritize response, meaning that aid may not always be available
  - Insurance company aid is typically based on policy coverage of an incident
    - Some initial assessment aid may be generally available
  - Hire on-demand presumes resource availability

Framework area: private enterprise

- Businesses of all sizes and business-like entities (revenue-based non-profits, etc.)
- Key considerations:
  - Need to continue producing revenue
  - Continuity of operations in support of customers
  - Goodwill / trust in business – impact depends on how the enterprise is trusted
  - Operational impairment creates financial impairment (revenue and ability to borrow)
- Risks areas:
  - Non-compliance
  - Liability for interrupted operations
  - Liability for lost / stolen data

Framework area: government

- Entities which operate by virtue of statutory authority
  - May include entities which individuals / firms must interact with and those that they interact with on a discretionary basis
- Key considerations:
  - Public perception / trust – government entities typically allow public input in operations and must make changes in response to public frustration
  - Revenue / goodwill – some entities are used by choice and have similar considerations to businesses
  - Need to maintain critical public services – utilities, police, fire, hospitals, others
  - Potential need to support others (residents, businesses, etc.) during a crisis
- Risk areas:
  - Compliance
  - Potential revenue impact
  - Liability to constituents / suppliers / other parties

Framework area: academia

- Academic institutions such as schools, colleges, universities
- Key considerations:
  - Population of students requiring services during incident – potentially residential
  - Impact on broader services provided to community
  - May be expected to participate in broader emergency response during incident
  - Highly dependent on goodwill / trust
  - Operational impairment may create financial impairment
- Risks areas:
  - Non-compliance
  - Liability for interrupted operations
  - Liability for lost / stolen data

Framework area: individuals

- People acting in a personal capacity
- Key considerations:
  - Immediate impact to needed services – food, shelter, heating/cooling, etc.
  - Medium-term impacts – needed services, morale, reestablishing normal routines
  - Long-term impacts – career / job impacts, housing impacts, identity impacts
- Risk areas:
  - Very limited window for key service resumption after some types of incidents
  - Even properly responded to incidents can have long-term impacts
  - Individuals are potentially involved in bot personal response, and organizational response
  - Long term impacts must be considered in the short term

Bringing it together: framework

- Individual organizations consider:
  - Risks
    - Risks' impact
    - Risks' likelihood
  - Preparation and response
    - Best practices for operation
    - Response plans
- Plans should consider broader impact
- Individual organizations plans can feed into regional / larger scale plans

Bringing it together: framework

- Can’t assume that individuals have plans
  - Some may
  - Plans may be scope-limited, out-of-date or poorly thought out
- Must consider issues with organizational plans
  - Poorly designed / implemented
  - Different levels of detail
  - Lack of consideration beyond organization
  - Out-of-date
  - Estimation issues
  - Organizations may fail in crisis and thus not act on plans
  - Some organizations may not have plans

Bringing it together: framework

- Societal assessment is a summation of individual and organizational risks
  - Outputs of individual risk assessments
  - Consider factors not assessed by organizations (failure, etc.)
  - Consider plans' quality and related issues
  - Consider reliability of firms / individuals during crisis situation
- Useful to understand, even if the impact of risk assessor on individuals and organizations is limited
  - Potential to target aid at areas of high return
  - Better understanding of where issues may arise from
  - Better understanding of preparedness of organizations / individuals in region
  - Focus on this may cause organizations and individuals, who otherwise wouldn't have, to create their own plans
- Assess plans for critical weaknesses
- Assess plans for systematic weaknesses
- Look for areas where a single incident or closely related incidents may cause disproportionate impact.

Conclusion & future work

- Work on this framework is ongoing and focused on adding more detail / nuance and examples to it
- Built on key concepts of risk and emergency management
- Some issues will be broader than just cybersecurity issues
  - Within information technologies
  - Issues / incidents with a cybersecurity component
- These core concepts can be used right now by organizations and planners
- Growing reliance on electronic systems makes risk assessment critical

Thanks & Any Questions?

Contact: jeremy.Straub@ndsu.edu

Image from: Microsoft