

# Session #58

## Computer Data- Cracks and Leaks

Michele Iversen  
U.S. Department of Education



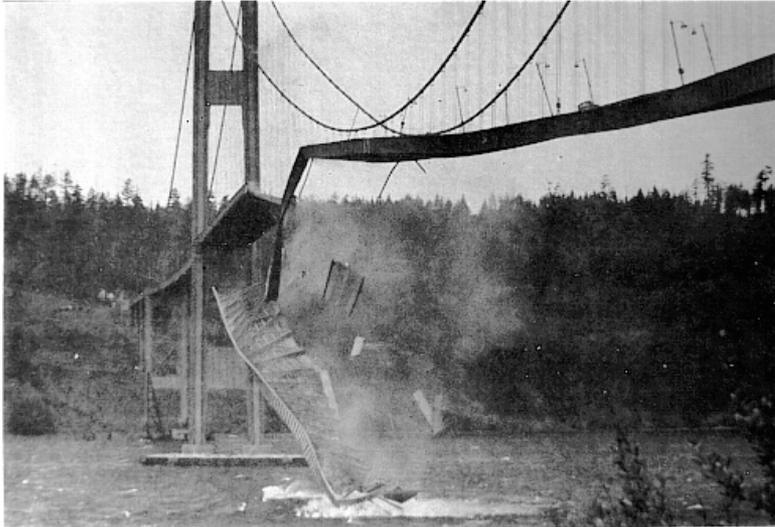
START HERE  
GO FURTHER  
FEDERAL STUDENT AID

# Cyber Security Landscape

- Networks upon networks
- Hierarchies of virtual and physical networks
- Range from tiny to large
- Many smart, small devices
- Highly interconnected
- Hybrid systems pervasive
- Sensor and control



# Engineering Challenges and Dangers



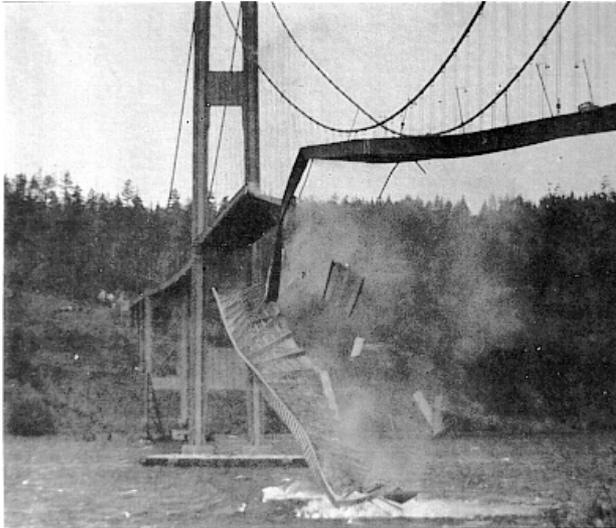
Many of the problems exhibited in today's bridges are due to a lack of adequate pre-construction engineering—a combination of naivete among owners regarding design challenges and an unwillingness to provide the necessary financial resources.



Three days after the disaster a structural engineer discovered a significant change of the original design of the walkways. This design change would prove fatal.

Investigators concluded that the basic problem was a lack of proper communication. The architect failed to review the initial design thoroughly, and accepted the developer's proposed plan without performing basic calculations that would have revealed its serious intrinsic flaws.

# Engineering Challenges and Dangers



While it's unclear whether principal engineer Leon Moisseiff, was aware of the problems plaguing other new bridges, he argued against cost-cutting adjustments to the original design and against initiatives that would detract from the bridge's appearance.

Many of the problems exhibited in the new bridges due to a lack of adequate pre-construction planning, engineering naivete and

challenges and an unwillingness to provide the necessary financial resources.

After the disaster a structural engineer discovered a significant change of the design of the walkways. This design could prove fatal.

Investigators concluded that the basic problem was a lack of proper communication. In the drawings prepared by the architects were only preliminary sketches but

and they had not been checked for initial design thoroughness, and accepted the developer's proposed plan without performing basic calculations that would have revealed its serious intrinsic flaws.

**A single flaw can topple the entire system.**



START HERE  
GO FURTHER  
FEDERAL STUDENT AID

# IT System Engineering Challenges and Dangers

- A broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depend on secure, reliable software
- Vulnerabilities in software can jeopardize intellectual property, consumer trust, and business operations and services
- It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or code of software

# IT System Engineering Challenges and Dangers

- Vulnerabilities in software, consumer services. A broad spectrum of infrastructure, from personal computers to commercial applications and services depend on secure, reliable software.
- It is estimated that 90% of reported security incidents result from design or code of



ardize intellectual  
ness operations and  
al applications and  
systems to  
pend on secure,

ported security  
fects in the

**A single flaw can topple the entire system.**



START HERE  
GO FURTHER  
FEDERAL STUDENT AID

# Building Security Into the System

- **Information Systems Security Engineering must be an integral part of the System**

## Engineering Lifecycle

- In the same manner that structural, safety and other types of specialties are utilized
- To ensure Security Requirements are developed, maintained and achieved alongside other requirements, not as separate, parallel or follow on process
- Failure to incorporate security requirements will result in marginalization of their importance or removal resulting in a less secure system
- Implementing security controls at later stages is not as simple as 'adding' them to the architecture
- Implementing security controls at later stages increase costs and risks



# Where Do We Start?

- Improved Software Engineering Practices
  - CWE/SANS Top 25 Most Dangerous Software Errors -  
<http://cwe.mitre.org/top25/#Listing>
    - SQL injection is the means to steal the keys to the kingdom from data-rich software applications
    - OS command injection, is where the application interacts with the operating system
    - The classic buffer overflow still harmful after all these decades
    - Cross-site scripting is the bane of web applications
    - Missing Authentication for critical functionality
  - **Open Web Application Security Project –**  
[https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)



# Develop Resilient & Survivable Systems

- Systems must:
  - Degrade gracefully
  - Maintain security under attack
  - Recover securely from fall-back mode
  - In worst case: fail secure

# Continuously Monitor for Vulnerabilities and Threat Activity

- Continuous monitoring is a risk management approach that maintains an accurate picture of an organization's risk posture, provides visibility into assets, and leverages the use of automated feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies
  - Know what is on your network
  - Identify your sensitive data or the “crown jewels” and where it resides in the system
  - Conduct real-time automated monitoring and analysis through implementation of tools that use Security Content Automation Protocols
- Develop a robust threat analysis and awareness program

# Through Integrated System Security Engineering We Can Build Safer Systems



...and minimize data cracks and leaks in the future.



START HERE  
GO FURTHER  
FEDERAL STUDENT AID

# Contact Information

We appreciate your feedback & comments.

Michele Iversen

Chief Information Security Officer

- Phone: 202-245-8287
- E-mail: [Michele.Iversen@ed.gov](mailto:Michele.Iversen@ed.gov)

# Session #58

## Computer Data – Cracks and Leaks

### ECMC Physical Data Theft: A Real-Life Case Study

Dick Boyle, ECMC Group  
President and CEO



# Incident recap

- Physical theft of two 200-lb safes from a locked room in our secured headquarters
- Safes included DVDs containing PII data on 3.3 million student loan borrowers
- Data recovered within 36 hours (although ECMC was not notified for nearly one month)
- Three people were charged and are currently serving time (none of them ever worked at ECMC)

# Actions taken

- Contacted law enforcement
- Activated our incident response plan
- Executed our communication plan
- Engaged our crisis team, which included key personnel from across the enterprise
- Worked closely with U.S. Department of Education
- Arranged for credit monitoring and identity theft protection services for borrowers

# Actions taken

- Established guiding principles for managing the crisis
  - CEO will lead from the front and take full responsibility
  - Be transparent and timely in communicating
  - Ensure the highest possible support for the borrower
  - Cooperate fully with law enforcement (FBI, BCA, OIG and local police)

# Actions taken

- Retained experts in data theft
  - Legal
    - Essential because the laws are complex regarding notification to consumers, attorneys general and other state agencies
  - Crisis communications/PR/media training
  - Physical security
  - Data security
  - Insurance broker and carriers



# Communication plan

Implemented a comprehensive plan to communicate with each of the following constituencies:

- Local law enforcement
- U.S. Department of Education
- Attorneys general/ required state agencies
- Board of Directors
- Congress and state government
- Departments of Education (in ECMC designated states)
- Borrowers
- Employees

# Communication plan

## Constituencies contacted (cont.):

- Collection agencies
- External auditors
- Financial partners
- Guarantors
- Industry organizations (FAAs, NASFAA, NCHELP, CBA, etc.)
- Insurance carrier
- Lenders/servicers
- Media/social media
- Schools

# Communication plan

- Involved legal in all communications
- Kept communications flowing—not once and done
- Retained a public relations firm experienced in crisis communications
- Developed key message points
- Pursued media training

# Borrower support

- Support focused on:
  - 3.3 million ECMC borrowers
  - All other federal student loan borrowers who would hear or read about the data theft
- Secured credit monitoring and identity theft protection services
- Established a 50-seat, 24/7 call center within 5 days of the theft

# Borrower support

- Utilized the executive management team to handle escalated inquiries, including phone calls
- Created a dedicated section of our website

# Security controls—what we learned

Despite being a security-minded organization...

**We learned that:**

- **You can never be diligent and thorough enough**
- **A breach will fundamentally change your organization**

# Security controls—what we learned

- Security must be ingrained into the culture of an organization—it starts with the CEO and senior management under strong Board oversight
  - Protecting customer data is the responsibility of every employee
  - All employees must understand policies—it is a continuous cycle (enhance, train, test, audit)

# Security controls—what we learned

- Stay diligent
- Know where your data is and ensure it is secure (PC/laptops, workstations, filing cabinets, portable media, systems)
- Review your business processes with a focus on the security of data

# Security control examples

## Physical controls

- 24/7 guards
- Proximity badge access controls
- Surveillance cameras
- Biometrics (data center)
- Alarmed doors/glass
- Clean desk audits
- Evacuation drills
- Penetrations tests
- Incident response tests

## System controls

- Firewalls
- Multifactor authentication
- Vulnerability assessments
- Laptop/desktop encryption
- Email encryption
- Secured print
- FISMA and PCI self assessments
- Data loss protection
- Antivirus/spyware
- System penetration tests
- Secure file transfer

# Policies

- Consolidated all policies into a single guide with oversight by one central policy team
- Policies must be easy to understand (include practical applications)
- Policies must be easily accessible (on the intranet)
- Continual reminders and training for employees
- Ensure each employee understands his/her role in protecting data

# 6 recommendations

1. Be alert – it can happen to you!
2. Ensure each employee understands his/her role in protecting PII data
3. Review your physical and data security controls
4. Know where your data is; ensure it is secure
5. Ensure your policies are easily accessible and understandable to employees
6. Be prepared in the event you are faced with a crisis



# Contact Information

If you have security-related questions for ECMC, please contact our Chief Security Officer, Ron Kuriscak.

Phone: 651-325-4085

Email: [rkuriscak@ecmc.org](mailto:rkuriscak@ecmc.org)