

# Cybersecurity for Project Managers

# Quick Intro

---

**Presented by Tim West**  
Field CTO, deepwatch

**Professional Background: ~15 Years Cyber**

- ~4 Years building deepwatch
- 5 Years Consulting for F2000s
- 5 Years Information Security @ ESI
- Prior experience as IT professional

**Exciting Engagements:**

- Acting CISO for largest HIPAA Fine (~\$5M)
- Security for manned-space missions for Tony Stark Company
- Multiple engagements for FANG companies



# Agenda

---

1. Talk about Cybersecurity Trends (Problem)
2. Explain the Recurring Gap Areas and How Project Managers Can Improve Your Organization's Cybersecurity (Solution)

# Cybersecurity Problems

# Gratuitous Headlines!

---

## The Accellion Breach Keeps Getting Worse—and More Expensive

**WIRED**

What started as a few vulnerabilities in firewall equipment has snowballed into a global extortion

### A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

April 16, 2021 · 10:05 AM ET

Heard on [All Things Considered](#)

## One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators





# 2021 Verizon Data Breach Investigation Report

29,207 Security Events Reported --- 5,258 confirmed data breaches

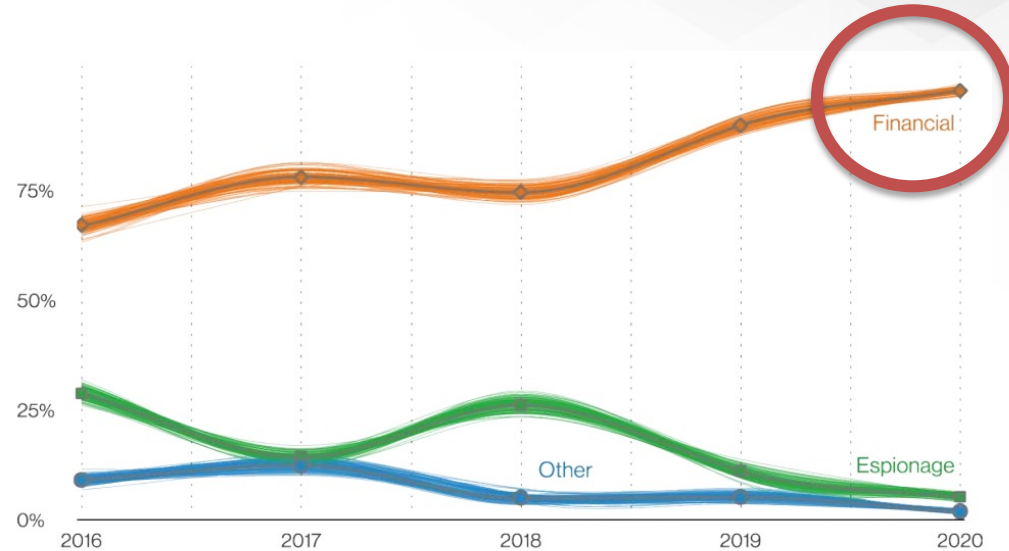
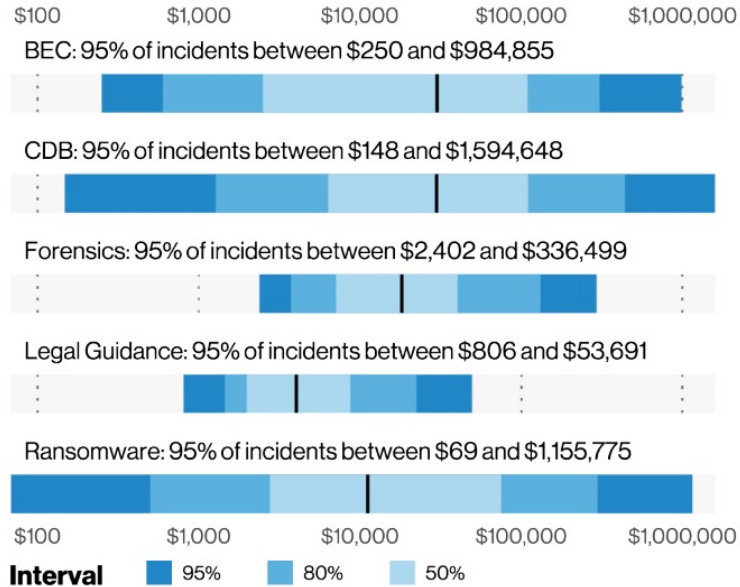
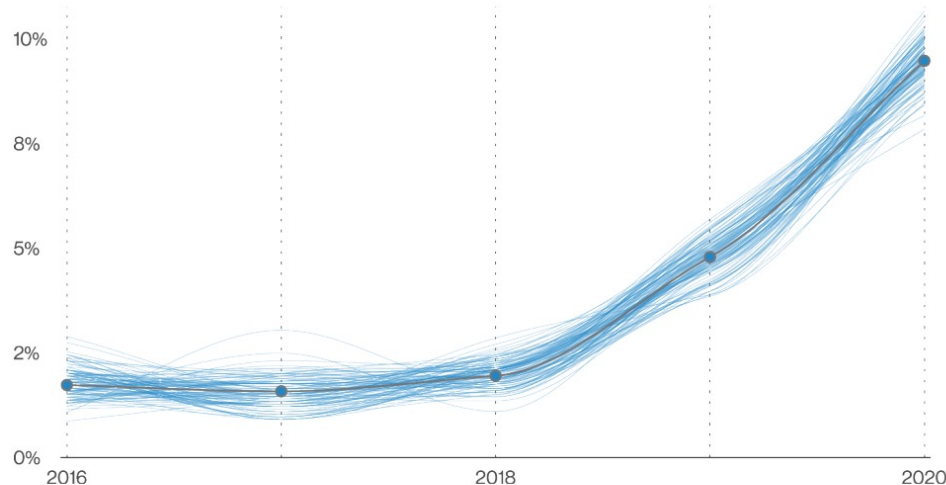


Figure 15. Top threat actor motive over time in breaches



# Ransomware Basics



**Figure 83.** Ransomware in breaches over time

## 5 STAGES OF CRYPTO-RANSOMWARE

### 1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.



### 2 CONTACTING HEADQUARTERS

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.



### 3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.



### 4 ENCRYPTION

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.



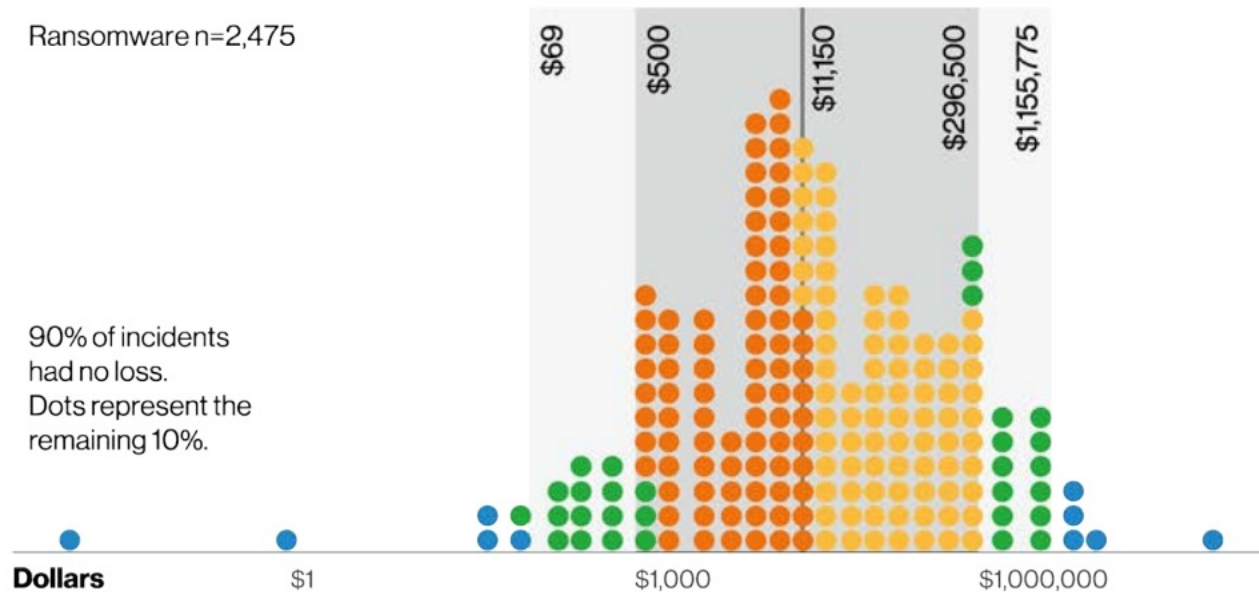
### 5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.





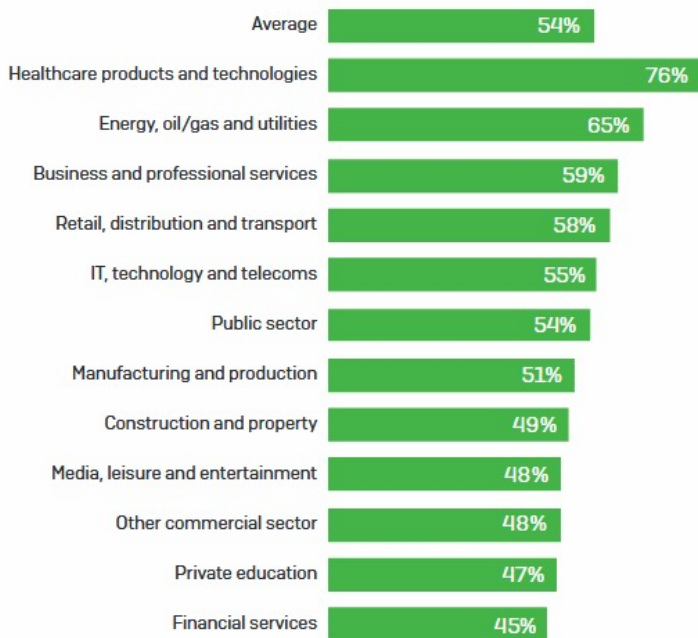
# Ransomware Financial Impact



**Figure 40.** Loss by incident type  
Each dot represents 0.5% of incidents

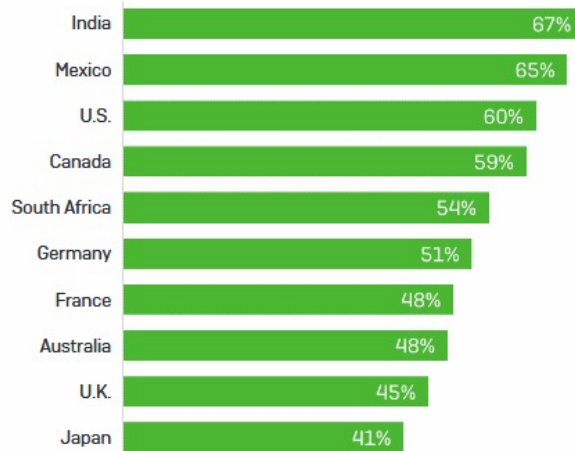
# 2700 Surveyed IT Professionals

## Hit by ransomware, by sector



*% of organizations that had been hit by ransomware in the previous 12 months, by sector*

## Hit by ransomware, by country



*% of organizations hit by ransomware in the previous 12 months*

# The Takeaway

---

Attackers are mostly opportunistic, they focus on vulnerable targets (technologies)

As such, the “I’m not an interesting target” perspective is a fallacy

Attackers are focused on **financial gains**, not destruction or fame and find you **after** they’ve gotten a means to extort you

# What Problems Can You Help Solve?

# 1 Significant Areas for Improvement

---

#1:

Cybersecurity Investments Are  
Poorly Implemented and  
Maintained

# Microsoft has a \$20 billion hacking plan, but cybersecurity has a big spending problem



## KEY POINTS

- Microsoft is quadrupling its cybersecurity investment to \$20 billion over the next five years.
- One of the reasons for the big investment cited by Microsoft president Brad Smith in a CNBC interview this week speaks to a Catch-22 in the cyber arms race: the increased spending in recent years by public and private enterprises hasn't resulted in better protection against criminal hackers.
- The shortage of workers skilled in cybersecurity is one of the factors that has led to a situation in which companies are paying for products that in many cases they aren't even using.



# This is Reality

---

“We see this ALL the time in our customers,” David Kennedy, founder and CEO of Trusted Sec, wrote in a email. “These companies will buy products, but not include direct staff to support it or else they can’t get the internal funding approval to support it. So the cybersecurity investments are only half installed or not at all and just languish. They barely get any value.”

## 2 Significant Areas for Improvement

---

#2:

Cybersecurity Audits Have  
Questionable Results

# Aren't We All Regulated?

## Banks' False Sense Of Cybersecurity Will Be Shattered By Cloud Computing



Ron Shevlin Senior Contributor ©

Fintech

Observations from the Fintech Snark Tank

Forbes

### A False Sense of Cybersecurity

It's hard to believe, but bank executives' concerns regarding cybersecurity are *declining* (that isn't a typo).

According to Cornerstone Advisors' [What's Going On in Banking](#) studies, nearly half of bank executives put cybersecurity on their list of top three concerns for 2018. That percentage declined to 36% in 2019 and dropped even further to 21% in 2020.

## HIPAA Audits May Give False Sense of Security



HIPAA  
JOURNAL

Home

Healthcare Data Privacy

HIPAA Audits May Give False Sense of Security

# Circular Logic

---

- We're all undergoing more audits with a cyber component:
  - SOX
  - HIPAA/HITECH
  - PCI
  - NYDFS
  - GLBA
  - GDPR/CCPA
  - FFIEC
  - FISMA/FEDRAMP/NIST RMF
- See previous Breach Data. Not well studied due to sensitivity of topic (opinion)

# Summary

---

- Project managers are regularly engaged to implement new technologies/processes or to assist in fulfilling audit requests or regulatory needs
- Project Managers can play a key role in the success of both of these areas

# How Project Managers Can Help



# How Project Managers Can Help

---

## 1. Get Attached to Cyber Projects

## 2. Create Measurable Success Criteria for any Cyber Project:

1. Network Security – % of enforcement features configured
2. Identity & Access Management – users enrolled and configured correctly
3. Endpoints – agents deployed **and** policy enforcements enabled
4. Cloud – configured use cases for all in-scope environments

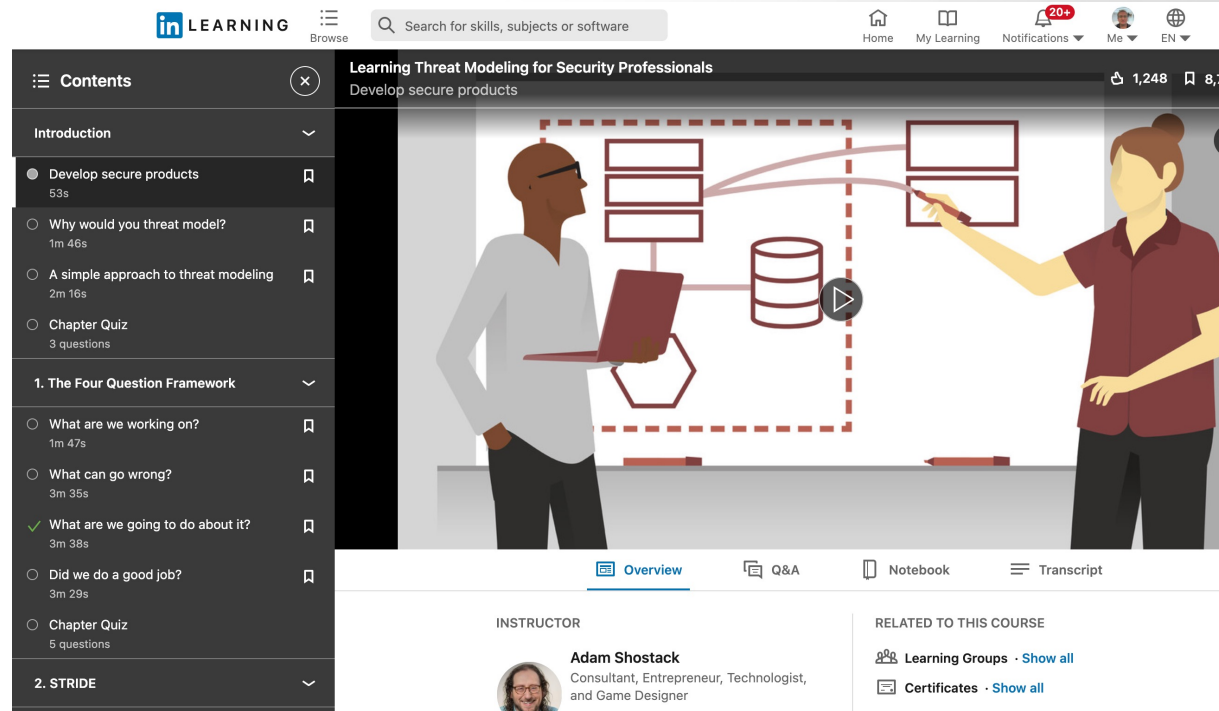
## 3. Define Specific Evidence as Project Close Requirement

1. Engineer X has to show data on above data points
2. Test criteria are even better - we prove out cyber projects in a lab/proof of concept then roll out to the organization but never validate it worked at scale

# How Project Managers Can Help

## 4. Get Familiar with Threat Modeling:

Threat modeling is a framework for thinking about what can go wrong, and the foundation for everything a security professional does.



The screenshot shows the LinkedIn Learning interface for the course "Learning Threat Modeling for Security Professionals". The course title is "Develop secure products". The left sidebar contains a table of contents with the following items:

Item	Duration
Introduction	
● Develop secure products	53s
○ Why would you threat model?	1m 46s
○ A simple approach to threat modeling	2m 16s
○ Chapter Quiz	3 questions
1. The Four Question Framework	
○ What are we working on?	1m 47s
○ What can go wrong?	3m 35s
✓ What are we going to do about it?	3m 38s
○ Did we do a good job?	3m 29s
○ Chapter Quiz	5 questions
2. STRIDE	

The main content area shows a video player with a play button. The video thumbnail depicts two people in a meeting, one pointing at a diagram on a screen. The diagram shows a server rack, a database, and a play button. Below the video player are navigation tabs: Overview, Q&A, Notebook, and Transcript. The instructor information is as follows:

**INSTRUCTOR**  
Adam Shostack  
Consultant, Entrepreneur, Technologist, and Game Designer

**RELATED TO THIS COURSE**  
Learning Groups - Show all  
Certificates - Show all

# How Project Managers Can Help

## 5. Learn Modern Security Principles

Beyond threat modeling, there's a number of modern techniques that help build security into the design of projects:

- Devsecops (securing devops practices)
- Cloud security (see Cloud Security Alliance work)
- FAIR (Factor Analysis of Information Risk); good for doing quantitative analysis of “will this security control actually solve a business problem”
- Zero Trust Security models: effectively rethinks security in a remote world



# How Project Managers Can Help

---

## 6. Recognize All Capex and No Opex Means No Security Value

1. Cybersecurity always has a “run” component but projects rarely fund it
2. Investments without a “run” investment will achieve 0 value
3. Two options: headcount or third party; choose one

## 7. Accept That You Will Struggle to Implement This Well –

1. Seriously, you **will fail to implement anything** worth \$100K or more with internal resources
2. Pay for Implementation Services; No conflict of interest but seriously, 100% of past clients have at least 1 cybersecurity product incorrectly implemented; some have all (millions spent but limited/no value)

# How Project Managers Can Help

## 8. Training is Still a Big Deal

1. Rarely do projects include training in their BOM
2. Buy it! Negotiate it in! It's <5% of your project spend
3. I can guarantee a new product in your environment will have at most 1 sophisticated user
4. Include completed training in Success Criteria

### ESG & ISSA RESEARCH REPORT

## The Life and Times of Cybersecurity Professionals 2021

- **Most organizations are impacted.** This year, 57% of respondents said that their organizations have been impacted by the global cybersecurity skills shortage. Among those who reported being impacted, 62% said that the skills shortage has increased the workload on existing staff; 38% said that new security jobs remain open for weeks or months; and 38% said that the skills shortage has led to employee burnout and employee attrition. This situation is difficult and unsustainable.
- **The skills shortage is not improving.** Forty-four percent of survey respondents believe the cybersecurity skills shortage (and its impact) have gotten worse over the past few years, while 51% say it's about the same today as it was over the past few years. Sadly, only 5% believe the situation has gotten better.

# How Project Managers Can Help

---

## 9. Time is Not On Your Side

1. Cyber projects get funded after bad things happen
2. Executives are antsy to get things done because Board pressure
3. Solution 1: seek outside help; get or research partnerships in advance
4. Solution 2: manage scope hard to ensure value attainment & report up

## 10. All Your Vendor Management Skills Will Help You

1. 4 of my Topics so far have mentioned potentially seeking outside help
2. Improve your vendor management/sourcing skills
3. Brush up on "third party risk" as it relates to cyber



# How Project Managers Can Help

---

## 11. Communications Plans Win Cyber Projects

1. Cyber projects are hard, disruptive, complicated, and costly
2. If cyber projects are sensitive, keeping executives engaged is key
3. The more you manage up, the more success you'll find in getting and achieving support through the hard times (change windows/testing)
4. Beyond communicating up, stakeholders that have to “do the work” are the other obstacle to success; giving them a good idea of your WBS early so they can allocate resources will be key when it comes to implement

# How Project Managers Can Help

---

## 12. Regarding Audits

1. Seek executive buy-in to aim higher than the compliance goal  
Example:

PCI DSS Requirement 5 states that **you must protect all systems against malware and regularly update antivirus programs.** ... Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers). Ensure that all antivirus mechanisms are maintained. Oct 28, 2019

2. Better approach: Project Charter includes the specific features and configurations to ensure that XYZ security threats (ransomware) are enabled and validated as part of the project

# How Project Managers Can Help

---

## 13. Even Better for Audits

1. Consider technical testing for any elements deemed critical to the business (really for any security control implementation)
2. Third party (internal/external) can test the environment after implementation
3. Bake in time for the remediation of the testing (you spend 6 months planning, procuring, implementing, testing) then 1 week to fix the finding? Even with modern techniques baked in up front, defects will occur and you will still need to fix things if you properly test what you do.

# In Summary

---

Project Managers **can and should** play a critical role in improving cybersecurity in our organizations and can positively impact the breach statistics shared here

Tim.west@deepwatch.com

[linkedin.com/in/timothywest](https://www.linkedin.com/in/timothywest)