

# FYI in 45 Cyber-Security: Are you ready?

Panelists:

Jim Livermore

Dave Adams

Moderated by:

Andrew Beaton

*January 25, 2018*



**CDM  
Smith.**

# Today's discussion will focus on

- ▶ What are the risks, and where are they coming from?
- ▶ How to mitigate the risk of a security incident.
- ▶ How are we designing systems to make them more secure?

# Our Panel

## Panelists



**Jim Livermore**  
Global Cyber-Security Architect



**Dave Adams**  
Automation Project Manager

## Moderator



**Andrew Beaton**  
Moderator



What Are The Threats?

# 6 Types of Hackers



Ethical Hackers



Malicious Hackers



Hacktivists



State/Nation  
Sponsored Hackers



Corporate Hackers



Cyber Terrorists

# High Risk Data



Financial  
Account  
Information




Contractual &  
Litigation  
Information



Business & Real  
Estate Deals



Personal Data



Control Systems  
Data/Access



Intellectual  
Property



Design Data

Bowman Dam, Oregon



# Bowman Ave Dam, New York



# “Kemuri Water Company”

- ▶ 2016
- ▶ Syrian-linked hackers infiltrated a water treatment plant
- ▶ Systems (ICS & Business) ran on a single server
- ▶ Chemical dosing and changes to alter flow control
- ▶ 2.5 million customer records accessed
- ▶ Hundreds of Programmable Logic Controllers exposed



What Are The Entry Points?

# Top Causes of Cyber-Security Breaches

## #1 Phishing

- ▶ Loss/Theft of Device
- ▶ Social Engineering
- ▶ Abuse by malicious insider/former employee
- ▶ Operating system and application vulnerabilities
- ▶ External attack targeting business partner or third party

What Are The Consequences,  
And What Responsibilities Do  
Clients Have?

# 2017 Average Cost per Breached Record



\$380

Medical Records



\$245

Student/Educational  
Records



\$71

Public Sector Records

# 2017 Data Breaches



918

Reported Data  
Breaches



1.9  
billion

Records involved  
in theft



\$141

Average cost incurred for  
each stolen record

# Some companies affected in 2017

**EQUIFAX®**



**WHOLE  
FOODS  
MARKET**



**DocuSign®**



**SAKS  
FIFTH  
AVENUE**



Booz | Allen | Hamilton

**KASPERSKY<sup>lab</sup>**



**Deloitte.**



**Verifone®**

# Standards and Regulations

- ▶ Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity
- ▶ Presidential Policy Directive PPD-21, Critical Infrastructure Security and Resilience
- ▶ NIST 800-53, Security and Privacy Controls for Information Systems and Organizations
- ▶ NIST 800-82, Guide to Industrial Control Systems Security
- ▶ ISO27001, Information Security Management System
- ▶ AWWA Process Control System Security Guidance for the Water Sector
- ▶ AWWA J100-10, Risk and Resilience Management of Water and Wastewater Systems
- ▶ ISA-62443(ISA-99), Security for Industrial Automation and Control Systems
- ▶ CISQ Automated Source Code Security Measures
- ▶ NERC CIP Version 5, Critical Infrastructure Protection Cybersecurity Standards

# How Do We Mitigate The Risk of Security Incidents?

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education



Assign Responsibility

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education



Assign Responsibility



Patch Everything!

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education



Have a Plan in Place



Assign Responsibility



Patch Everything!

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education



Have a Plan in Place



Assign Responsibility



Monitor Environment



Patch Everything!

# 6 Steps to Mitigating the Risk of a Security Incident



Training and Education



Assign Responsibility



Patch Everything!



Have a Plan in Place



Monitor Environment



Test the Incident Response  
& Recovery Process

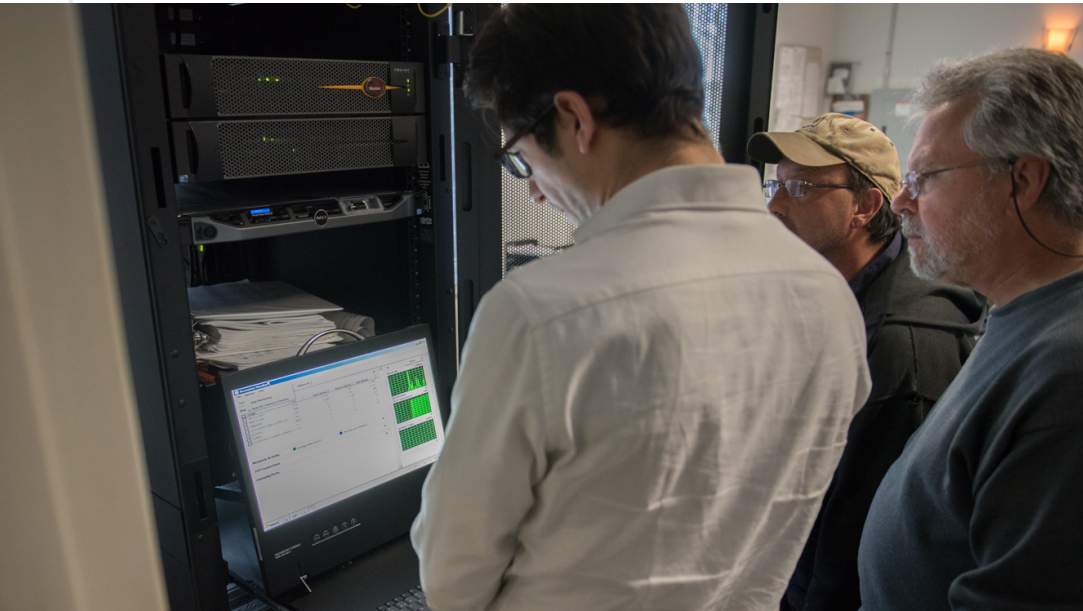
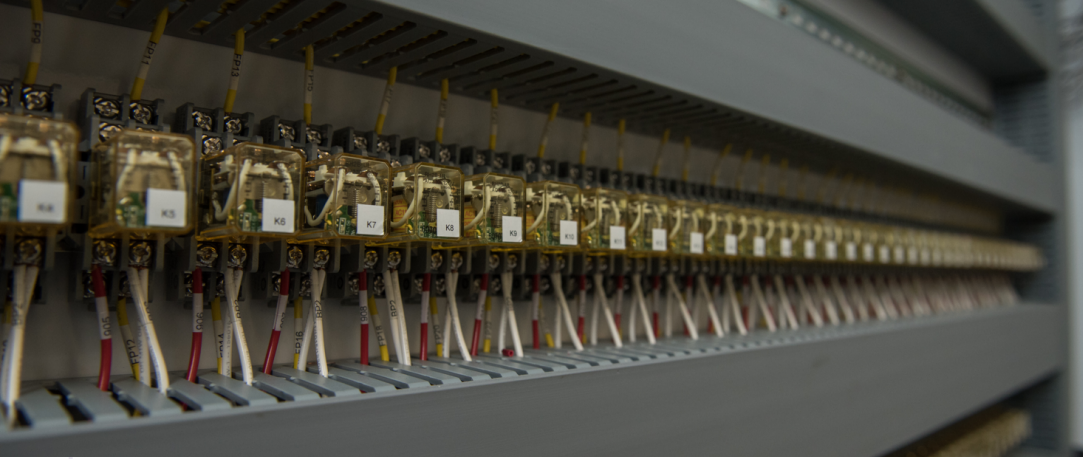


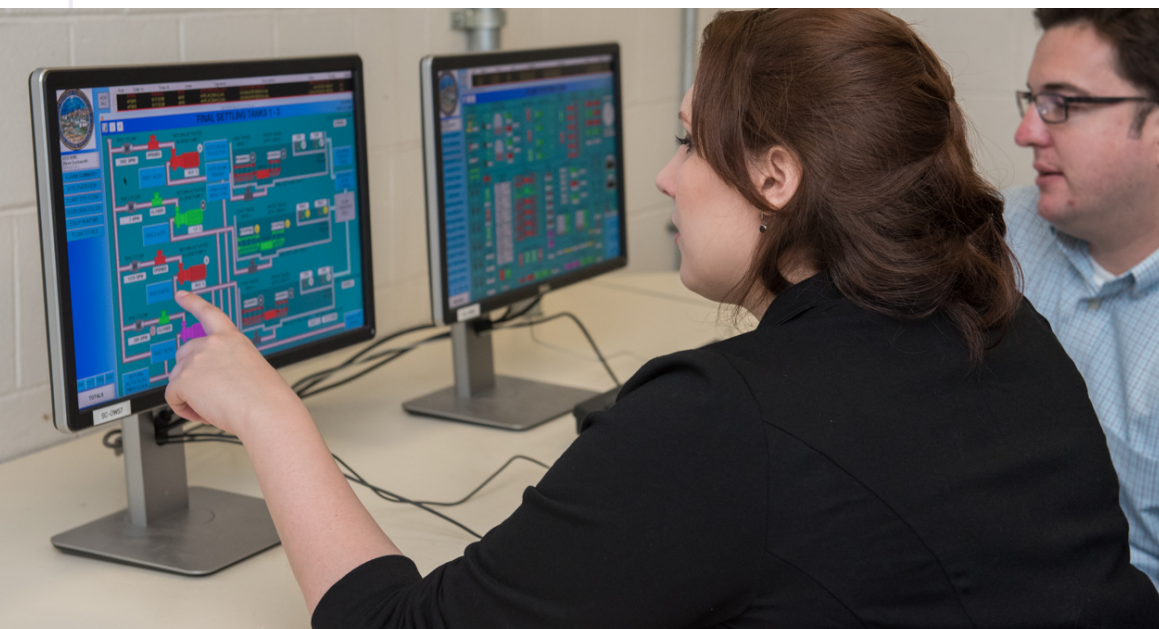
# Foundational Tools to Help Mitigate Risk

- ▶ Network Management & Mapping
- ▶ Firewalls
- ▶ Intrusion Detection/Network Security Monitoring
- ▶ Vulnerability Scanners
- ▶ Access Management
- ▶ Security Information and Event Management
- ▶ Incident Handling and Forensics
- ▶ Virus/Malware Protection
- ▶ Data Backup/Disaster Recovery
- ▶ Physical Security

The background is a dark blue gradient with a complex, glowing pattern of white and light blue lines and dots, resembling a circuit board or a network map. The lines are thin and interconnected, with small, bright circular nodes at various points. The overall effect is a high-tech, digital aesthetic.

# Designing For Cyber-Security





# Grafton, MA WWTP



# What Do You Do When an Incident Occurs?

# Security Breach Checklist



Execute Rehearsed Incident Response Plan

# Security Breach Checklist

- ☒ Execute Rehearsed Incident Response Plan
- ☒ Contain the Issue

# Security Breach Checklist

- ☒ Execute Rehearsed Incident Response Plan
- ☒ Contain the Issue
- ☒ Identify the Root Cause

# Security Breach Checklist

- ☒ Execute Rehearsed Incident Response Plan
- ☒ Contain the Issue
- ☒ Identify the Root Cause
- ☒ Notify the Authorities

# Security Breach Checklist

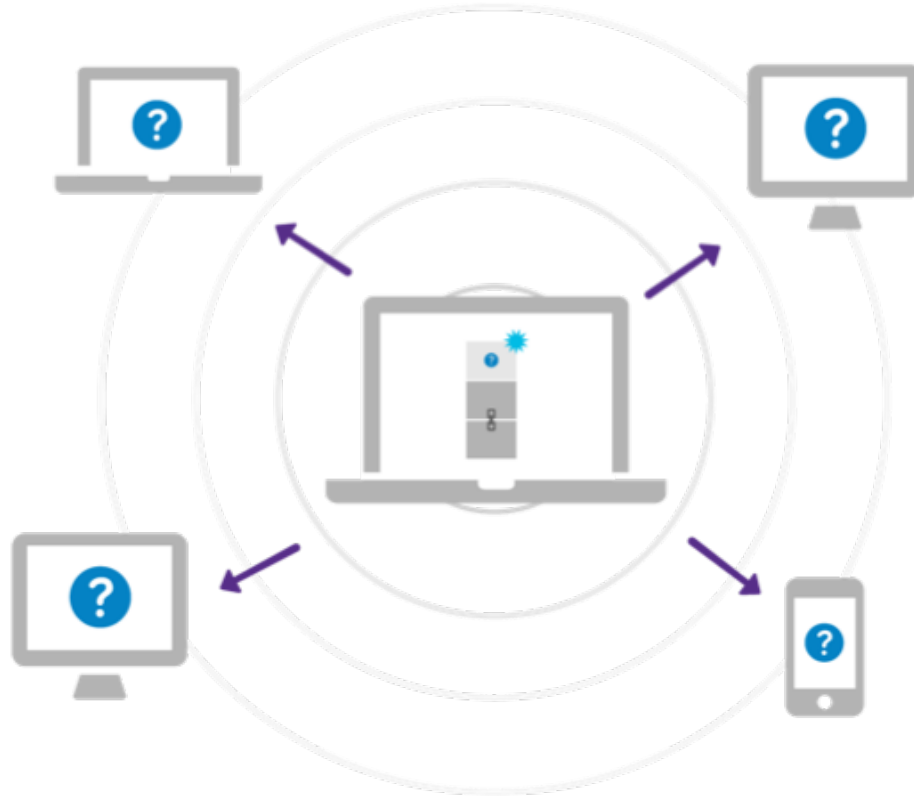
- ☒ Execute Rehearsed Incident Response Plan
- ☒ Contain the Issue
- ☒ Identify the Root Cause
- ☒ Notify the Authorities
- ☒ Communicate to the Public

# Security Breach Checklist

- ☒ Execute Rehearsed Incident Response Plan
- ☒ Contain the Issue
- ☒ Identify the Root Cause
- ☒ Notify the Authorities
- ☒ Communicate to the Public
- ☒ Begin Recovery

# Looking to The Future: Blockchain

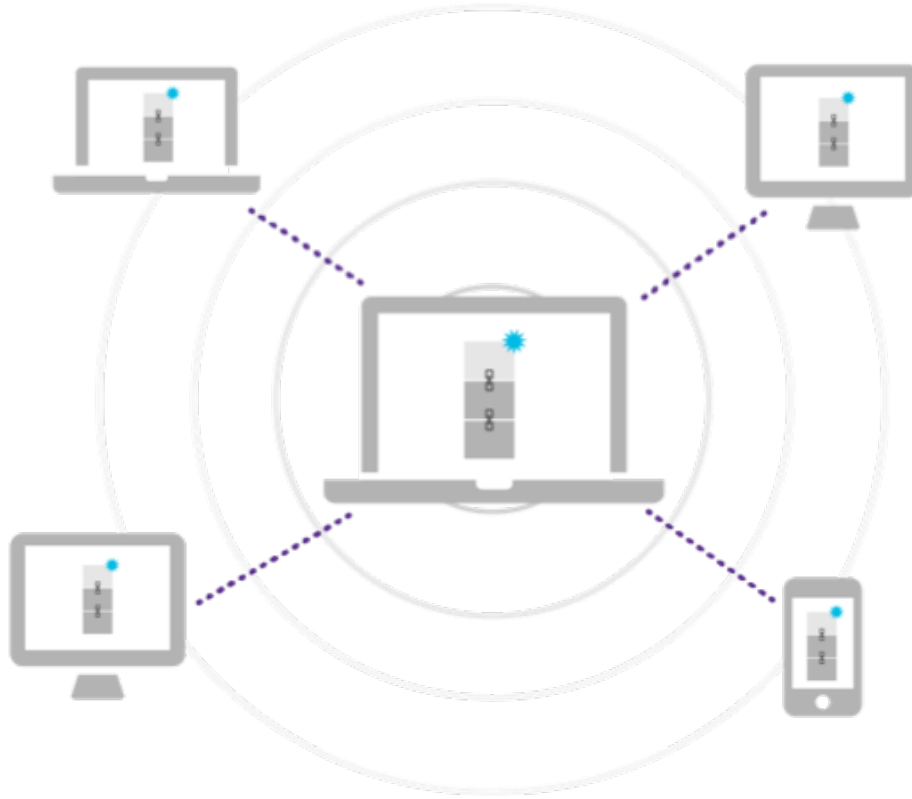
# What is Blockchain?



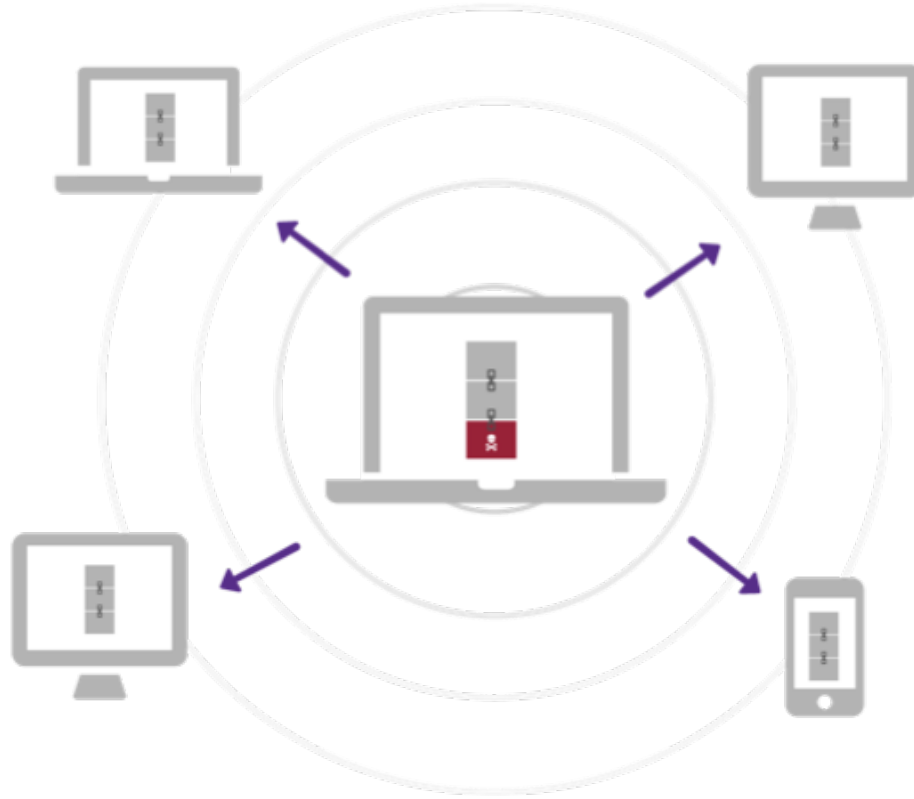
# What is Blockchain?



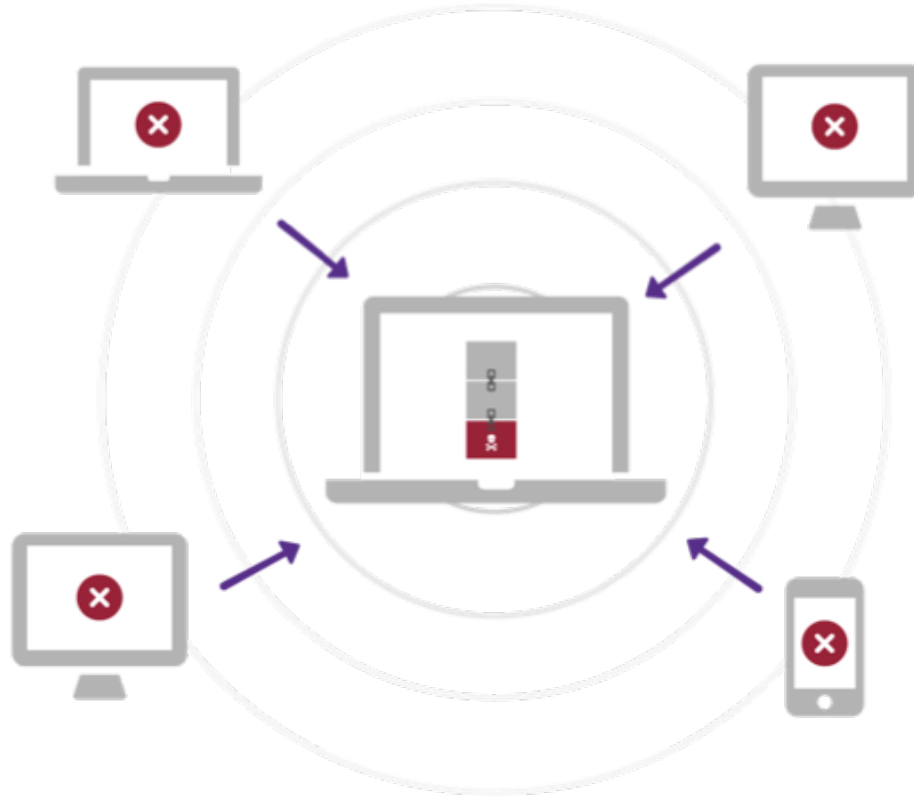
# What is Blockchain?



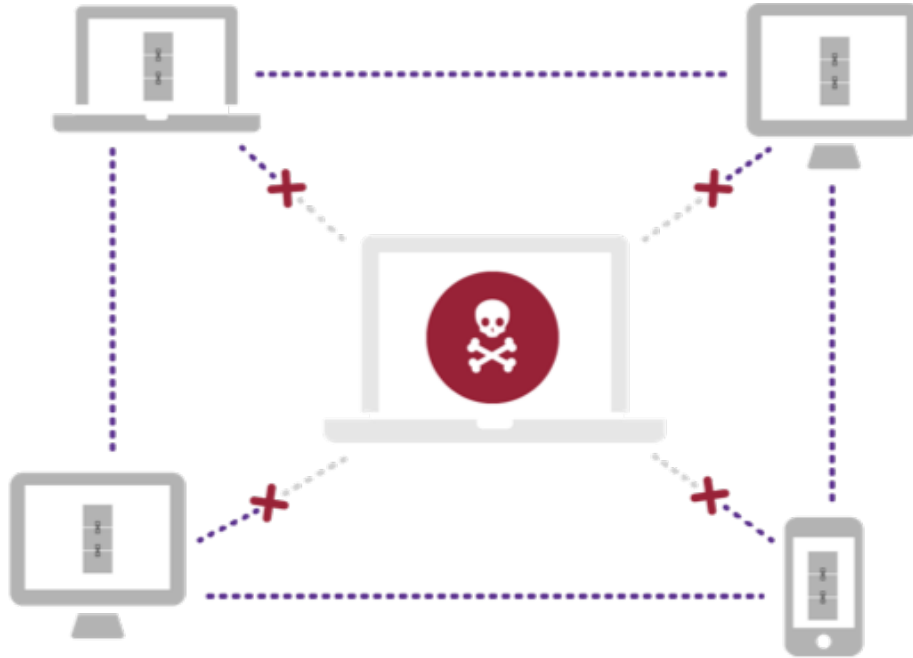
# What is Blockchain?



# What is Blockchain?



# What is Blockchain?



# Blockchain in a Community



# Blockchain in a Community





Thank You