Not IF, but **WHEN** you have a cyber attack are you prepared?... Staying ahead of the bad guys!
Get Ahead of Cyber Crime

Anticipating Cyber Attacks Is The Only Way To Be Ahead Of Cyber Criminals

Presented by
John Kelley and Eric Eder

Note to Reviewer
Much of this document is specific to Sequris Group information systems, policies, procedures, and IT security posture. As such, the contents of this presentation are classified as CONFIDENTIAL and cannot be copied, reused, or distributed without express written authorization from Sequris Group.
About Sequris

- Established in 1996
  - More than 700 clients
  - Over 2,500 projects completed
- National footprint
  - HQ in Royal Oak, Michigan
  - Sales and service offices
    - Royal Oak, Michigan
    - Denver, CO
    - Phoenix, Arizona
  - SOC – Royal Oak
  - Data Center – Phoenix
Current State of the Union:
Survey June 2016 by Dark Reading and Black Hat USA conference predominantly large companies with 60% working with 1,000+ employees

- IT professionals expect there is a 40% chance a security breach will occur in the next 12 months
- Too many rapidly evolving threat agents
- A rise in social engineering attacks directly at targeted organizations
- What to do about Ransomware
- Resources for organizations to deal with all of the cybersecurity concerns
What are your Top Executive’s concerns?

- Attacks directly targeted at our organization
- Effort to stay in compliance
- Phishing social network exploits social engineering
- Accidental data leaks by end-users
- Effort to measure the organization’s security posture
- Data theft by insiders
- Mistakes or attacks that cause organization to lose compliance with industry regulations
- Espionage
- Ransomware
Ransomware

- Sam returns from lunch and is surprised to see an error on his computer
- He doesn’t remember clicking on anything or visiting any inappropriate sites

Your computer has been encrypted

The hard disks of your computer have been encrypted with a military grade encryption algorithm. It’s impossible to recover your data without a special key. This page will help you with the purchase of this key and the complete decryption of your computer.

Your data will be permanently destroyed in:

23 hours 58 minutes 49 seconds
Help

- Sam spends several hours trying to figure out the issue on his own and then reluctantly contacts the company help desk
- The help desk technician immediately responds
Escalation

- Over the course of the next 6 hours the help desk receives 11 more data encryption incidents
- One incident is reported from the windows systems administrator
- Multiple users are now reporting that they are unable to access files on shared network drives
With only 6 hours to go...
Who should be engaged?
Will your organization pay the ransom?
Has any data been exfiltrated?
Is your organization required to report a breach?

06 hours 15 minutes 29 seconds
Cyber Crimes are Intrusive and Frequent

The benchmark sample experienced 50 discernible and successful cyber attacks per week, which translates to more than one successful attack per company per week.

Benchmark Study of U.S. Companies; Conducted by Ponemon Institute 2013
Incident Response & Remediation is Costly

Bar chart showing the cost of various types of cyber incidents for U.S. companies, conducted by Ponemon Institute in 2015.

- **Malicious Insiders**: $150,000
- **Denial of Service**: $140,000
- **Web Based**: $100,000
- **Phishing**: $90,000
- **Malicious Code**: $70,000
- **Other**: $50,000

Benchmark Study of U.S. Companies; Conducted by Ponemon Institute 2015
The Trend is NOT our Friend at the moment

Resolution (days) + 229%

# Attacks +46%

Benchmark Study of U.S. Companies; Conducted by Ponemon Institute 2015
Where do you stand now?

Opportunity for Improvement

Explicit

Risk Tolerance & Security Policy (Requirements)

Chaos

Reactive

Security Operations (People, process, technology)

Predictive

Optimize

Proactive
Best Practices: Steps to Optimization

1. Establish Control Objectives
   - Business Drivers
   - Client Requirements

2. Engage Priority Action Map
   - Clear Next Actions
   - Optimal Resource Allocation

3. Measure Effectiveness
   - Increase Efficiency
   - Reduce Cycle Time
Best Practice Approach: Applied to CVS 20 Critical Controls

Q|Frame™ Dashboard

- Inventory of Authorized Devices
- Inventory of Authorized Software
- Secure Configurations for Computers
- Secure Configurations for Network Devices
- Boundary Defenses
- Analysis of Security Audit Logs
- Application Software Security
- Controlled Use of Administrative Privileges
- Controlled Access Based on Need to Know
- Vulnerability Assessment and Remediation
- Account Monitoring and Control
- Malware Defenses
- Network Access Control
- Wireless Device Control
- Data Loss Prevention
- Secure Network Engineering
- Penetration Tests and Red Team Exercises
- Incident Response Capability
- Data Recovery Capability
- Security Skills Assessment
- Secure Network Engineering
- Penetration Tests and Red Team Exercises
- Incident Response Capability
- Data Recovery Capability
- Security Skills Assessment

Best Practice Approach: Applied to CVS 20 Critical Controls
Q|Frame™ Applied to Critical Controls

| Q|Frame™ Dashboard |
|---|
| **Q|Frame™ Dashboard** |
| **1. Inventory of Authorized, Unauthorized Devices (1.33)** |
| **2. Inventory of Authorized, Unauthorized Software (1.50)** |
| **3. Secure Configurations for Computers (2.98)** |
| **4. Secure Configurations for Network Devices (1.14)** |
| **5. Boundary Defenses (3.0)** |
| **6. Analysis of Security Audit Logs (2.97)** |
| **7. Application Software Security (1.0)** |
| **8. Controlled Use of Administrative Privileges (3.07)** |
| **9. Controlled Access Based on Need to Know (1.50)** |
| **10. Vulnerability Assessment and Remediation (.90)** |
| **11. Account Monitoring and Control (4.0)** |
| **12. Malware Defenses (1.42)** |
| **13. Network Access Control (2.33)** |
| **14. Wireless Device Control (1.38)** |
| **15. Data Loss Prevention (3.57)** |
| **16. Secure Network Engineering (3.1)** |
| **17. Penetration Tests and Red Team Exercises (1.0)** |
| **18. Incident Response Capability (3.0)** |
| **19. Data Recovery Capability (2.0)** |

Q|Frame™
Information Security Management System
The timeline outlines successive security enhancements across the organization. Some projects will overlap because of general information gathering, etc. Timelines are estimates; however, a .8 confidence factor is applied.
The **uncontrollable** information security threat – that you can **influence**…

- Limited Resources
- Limited Time
- Limited Money
Summary

- Conduct staff interviews
- Align control objectives with client requirements
- Perform gap analysis

- Clear tactics
- Commitment to timeline and action
- Visibility & attribution

- Roles & responsibilities
- Document processes
- Align metrics with program goals

- Reduce cycle time
- Increase efficiency
- Objective reprioritization
- Dashboard
- Contract ready
ROLE PLAY