Cyber Security with Real Experience

Mike Sadler, MBA, cyRM, Risk Advisor, VAST
John Kelley, Regional Sales Director, CyberForce|Q
Michael Sadler, MBA, CyRM
Risk Advisor, VAST
mikes@vastsolution.com

John Kelley
Regional Sales Director, CyberForce|Q
jkelley@cyberforceq.com
Agenda

• The Numbers
• What’s at Risk
• How Does a Breach Occur
• Front End Protection
• Back End Protection
• The Real Cost of a Cyber Incident
• Cyber Insurance
“Cyber crime is the greatest threat to every company in the world.”

Ginni Rometty
Former CEO IBM
“We had planned for the loss of an entire data center, the loss of key critical online services.

What we hadn’t planned for was the complete loss of everything.”

Don Jaycox, CIO, DLA Piper
What's at Risk

Data

Disruption

Dollars
How Does a Breach Occur?

Outside Attackers
• Hackers

Inside Threats
• Malicious insider

3rd Party Incidents
• Vendors being used
Front End Cyber Protection

John Kelley, Regional Sales Director, CyberForce|Q
THE CURRENT ENVIRONMENT

50M healthcare records exposed or compromised in 2021

$9.23M Average cost of a data breach in the healthcare sector in 2021

287 days average time needed by organizations to detect and contain a breach
VALUABLE INFORMATION SHARING REQUIREMENTS

- Quality of information (QoI)
- Quality of service (QoS)
- Installed base (i.e., number of end users)
- Timeliness
- Trust
- Cost
- Trusted communities
- Cyber Insurance
A security arrangement, political, regional, or global, in which each state in the system accepts that **the security of one is the concern of all**, and therefore commits to a collective response to threats to, and breaches to peace.
COLLECTIVE SOC ORIGIN

- Washington D.C. to State Capital
- Michigan Hospital Association (MHA), University of Michigan: Michigan Medicine, Munson Health, & CyberForce|Q
- Formation of the Healthcare Security Operations Center (HSOC)
COLLECTIVE SOC

- Criteria & timeline established for collective SOC model
- Successful, proven results in record time (6 months)
- Achieved through collective model
OPERATIONAL COMPONENTS

- Alert Triage & Response 24x7x365
- Incident Investigation & Resolution
- Information Aggregation, Analysis, & Reporting
- Incident Simulation & Training
IMPORTANT CONSIDERATIONS

FOCUSED
Combining cybersecurity expertise with contextual awareness

CUSTOMIZED
Customized playbooks and shared/automated intelligence keeps you ahead of the breach

RESPONSIVE
100% of security events are responded to in an average of **1.79 minutes**, 24x7x365
FLEXIBILITY IS KEY
EXAMPLE OF COLLECTIVE SUCCESS

**SIGNAL**
All participants feed signal to Collective

**INCIDENT**
Participant has incident, and response occurs accordingly

**SHARE**
Participants share threat data and lessons learned together

**DATA**
Anonymize and enrich data

**ACTION**
Deploy threat hunting in all environments

**FINDINGS**
Develop findings

**RESULTS**
Risk mitigations & recommendations are created for all
WE ARE STRONGER TOGETHER
Back End Cyber Protection
Mike Sadler, Risk Advisor, VAST
How Does Data Backup Work?

**RPO (Recovery Point Objective)**: Last point data is in usable format

**RTO (Recovery Time Objective)**: System is recovered

Time

Disaster Strikes

How far back?

How long to recover?

System is recovered

Last point data is in usable format

Recovery Point Objective

Recovery Time Objective
How to Get Started

1. Establish your group and your objectives
2. Inventory and prioritize
3. Develop strategies and procedures
4. Develop a communication plan
5. Document

KEEP CHECKING ON IT!
Real Cost of a Cyber Incident

Data Breach

- Breach coach/legal expenses
- Forensic expenses
- Notification and call center services
- Providing credit monitoring to victims
- Regulatory investigation

$783,596
Real Cost of a Cyber Incident

Ransomware
- Legal expenses
- Forensic expenses
- Ransom payment
- Data restoration
- Business interruption costs

$1,409,822
Real Cost of a Cyber Incident

Business Email Compromise
- Legal expenses
- Forensic expenses
- Theft of funds

$832,335
Cyber Insurance Coverage

First Party Coverages
- Incident Response
- Data Breach Coach Services
- Legal Services
- Forensics
- Notification Costs
- Credit Monitoring
- Public Relations

Third Party Coverages
- Ransomware
- Business Interruption
- Digital Data Recovery
- Privacy Liability
  - + Regulatory
  - + Payment Card
- Network Liability
- Media Liability
The Basics

- Multi-factor authentication
- Endpoint detection and response (EDR)
- Remote desktop protocol ports (RDP) – address vulnerabilities quickly
- Backup data frequently and securely
- Data management strategy
- Business continuity plan
- Strong passwords and password management
- Employee training
- Constant testing and updating
<table>
<thead>
<tr>
<th>Cyber Market Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance / renewals not being offered without security measures</td>
</tr>
<tr>
<td>Premium increases of 50% - 400%</td>
</tr>
<tr>
<td>Reduced limits of liabilities</td>
</tr>
<tr>
<td>Increased deductibles or retentions</td>
</tr>
<tr>
<td>Co-insurance penalties</td>
</tr>
<tr>
<td>Added exclusions</td>
</tr>
</tbody>
</table>
Front End Protection + Back End Protection + Cyber Insurance = Cyber Resilience

“Failing to plan is planning to fail.” – Benjamin Franklin
Question & Answer