Cybersecurity Masterclass

Access to Session Slides and Resources:

Staffing World App

staffingworld.net/materials2022

Use the Staffing World App to Rate This Session

Steve Akers
Chief Security Officer
Tech Lock Inc.

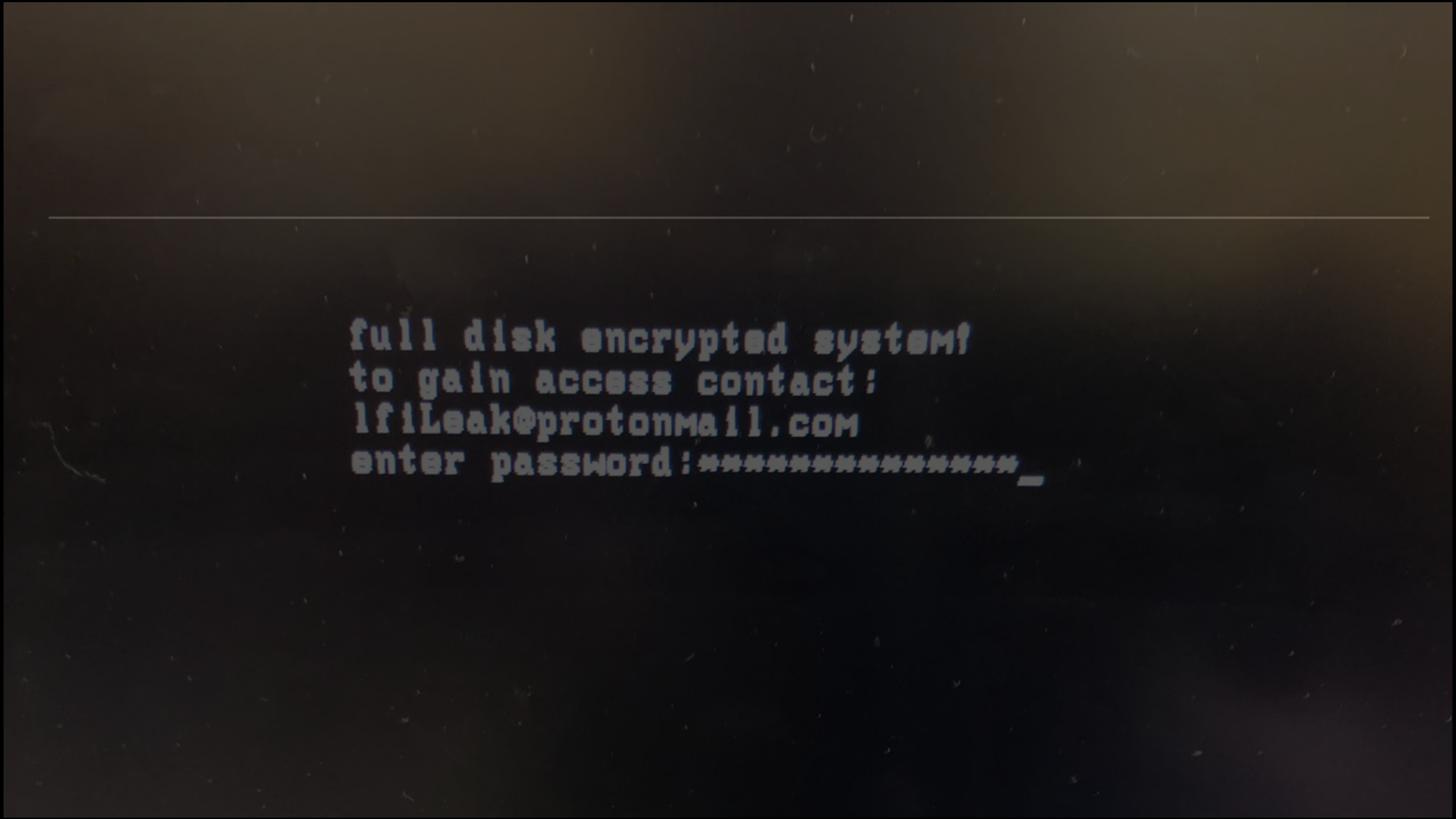
Mike Sisk
Vice President
Philadelphia Insurance Cos.

Michael Baker
Vice President &
Chief Information Security Officer
Kelly

Jorge Quintana
Chief Information Officer
Labor Finders International

Owen Meehan
Senior Vice President &
Chief Information Security Officer
Bullhorn

J. Quintana ▪ 2 15
J. Rondon 2 0
24/58
Flat
Forehand
49
MPH



```
full disk encrypted system!
to gain access contact:
lfiLeak@protonmail.com
enter password:**************_
```

What to have if you suffer a Cyber Attack?

- **Have full backups of all your systems**
- **Cyber Security Insurance**
- **Have an Incident Response Plan**
- **Put together a recovery team**
  - **Forensic Analysis Team**
  - **Negotiation Team**
  - **Restoration Team**
  - **Legal Team**

Tools to best defend from a Cyber Attack

- **Multi Factor Authentication**
- **Security Awareness Training**
- **Phishing Campaigns**
- **Penetration Testing**
- **Segmented IT Architecture**
- **Patch Management**
- **Vulnerability Management**
- **EDR (Endpoint Detection and Response)**
- **SIEM (Security Information and Event Management)**
- **UEBA (User and Entity Behavior Analytics)**
- **Security Operation Center (SOC)**
- **PMA (Privilege Access Management)**

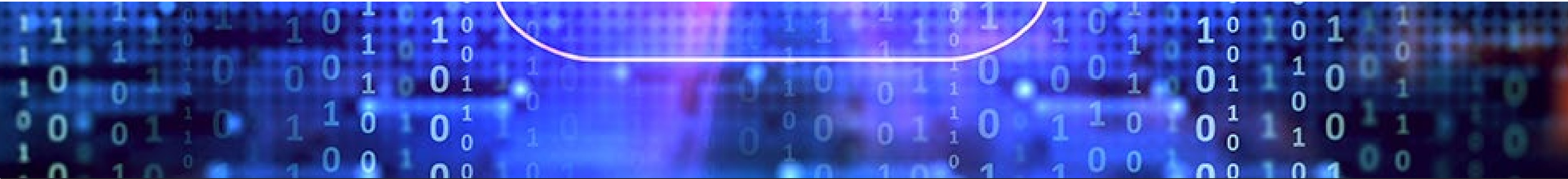
Tools to best defend from a Cyber Attack

- **Firewall**
- **Application Control**
- **URL/Content Filtering**
- **Intrusion Prevention System (IPS)**
- **Intrusion Detection System (IDS)**
- **Anti-Bot**
- **Anti-Virus**
- **Email Advance Security**
- **Content Awareness**
- **3-2-1 Backup**

Michael Baker

Vice President & Chief Information Security Officer

Kelly



Managing Data Security Across Multi-Platform Tech Stacks

Owen Meehan

Owen Meehan

SVP, Chief Information Security Officer, Bullhorn

Security Frameworks

- NIST Cybersecurity Framework
- ISO 27001 and ISO 27002
- SOC2
- NERC-CIP
- HIPAA
- GDPR
- FISMA

But what does that mean for me?

They Guide Us in Our Quest to Protect Everything, Everywhere, All at Once

WHO?

Identify who is accessing the Environment

WHAT?

The Assets in use by the Service

WHERE?

Location(s) where the Service is hosted

HOW?

Protective technologies and processes

WHO?

Identify who is accessing the Environment

Identifying the “Who”

*Knowing who **should** have access simplifies keeping others out*

Define Legitimate Users for All Environments	
Service / Platform Users	***Account types and levels***
Internal Users	***Role based access using “Least Privilege”***
Partners	***API Access*** ***Third Party Contributors***

WHAT?

The Assets in use
by the Services

Identifying the “What”

If you know your environment, you can protect it and identify risks

Inventory what it is you are protecting	
Hardware	***Servers, Networking Equipment*** ***3rd Party Devices***
Software	***3rd Party Software Components*** ***OS Versions***
Intellectual Property	***Code Repositories***
Data Types	***Customer Data*** ***Sensitive Corporate Data***

WHERE?

Location(s) where
the Service is hosted

Identifying the “Where”

Disaster Recovery, Business Continuity, and Security Ownership can depend on Location

Know your Data Flows and Protect them in ALL Environments

Is it Cloud Hosted?	***Servers, Networking Equipment*** ***3rd Party Devices***
Is it a Physical Data Center?	***3rd Party Software Components*** ***OS Versions***
Is it a Mixture of both?	***Code Repositories***
Are Regional Laws in effect?	***Customer Data*** ***Sensitive Corporate Data***

HOW?

Protective technologies and processes

“How” is it all Protected?

Security in Layers is Critical. Updating the Layers, and Evaluating Solutions for new Threats is Constant

So many Products Needed:

Identity Protections, SSO, MFA (Who)

- VPN, CASB, SASE (Who, What)
- Firewall, WAF, Cloud derivatives, DDoS Protections (Where)
- AV/EDR, Behavioral Analysis (Who)
- Asset/Vulnerability Management (What)
- Pen Testing, SDLC Security, Encryption at Rest (What)
- Encryption in Transit (Where, What)
- And many more!

How A Security Team Ingests It All

Consolidate and Automate

- SIEM Tools can centralize Logs
- Intelligence feeds and Platforms can help identify new and emerging threats
- 3rd Party Specialists can help test your controls with tabletops and active testing
- Augment your staff for specific functions like 24/7 monitoring
- Automate Investigations and Alert creation wherever possible.
- Create processes to clearly measure and prioritize risk.

Minimize the screens needed to identify and investigate suspicious events. Train for anything, and always be Testing.

What it all Leads To:
Risk Reduction!!

Our End Goals

- ○ Continuous Risk Reduction
- ○ Improved trust with our clients
- ○ Reacting quickly to new threats
- ○ Operational Stability
- ○ Business Value

Risk has a cost. EVERYONE wants to reduce that cost

It takes EVERYONE

Security is EVERYONE'S Job

- Executive Buy In is a must – this requires resources
- Employees need to know how to handle data securely and privately
- Privacy and Security by Design should be applied to all projects
- Consistency for all employees is required

Security and Privacy need to be familiar faces within a Company

TECH LOCK®

Cybersecurity Masterclass

Presenters

Steve Akers

CSO / CTO

- 25+ Year in Cybersecurity
- Veteran, Medic and Military Police
- Consulting, Software, Services, MSSP
- Serial Entrepreneur

John Lao

Security Analyst and Threat Hunter

- 2+ Years in Cybersecurity and IT

  Mr. Robot was his spark
- Loves hanging with the locals here in Vegas
- Into Fitness and Exercises Daily

TECH LOCK®

Headlines

North Korea Hackers Spotted Targeting Job Seekers with macOS Malware

Hackers are Highjacking Your Company’s Online Job Ads

Global Threat Actors Use the 'Great Resignation' to Target Job Seekers

We stopped these hackers who were targeting job hunters and crypto firms

Hackers Are Targeting Employers Looking To Hire

How Hackers are Using LinkedIn to Target Users With ‘Fake’ Job Offers

How and Why

- Just another Phishing Scheme
  - Same idea, different topic
- Captive Audience
  - Better Job
  - Remote Job
  - Shortage
- Targeted Attacks
  - Technical Vulnerability that allows exploit
- Opportunity to gather more information
  - Environment
  - Technical Footprint
  - Operational Details
  - Personnel

TECH LOCK®

Social Engineering Demo

Mitigating Risk with Cyber Insurance

Michael Sisk

Vice President - Underwriting

PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

ThinkPHLY

Talking Points

- What cyber covers
- State of the cyber insurance market
- Underwriting process and changes
- Underwriting process
- What makes a good Insured

What Cyber Covers

- Data loss
- Business interruption
- Lost profits
- Extortion and ransom payments
- Fines and penalties imposed by regulators
- Crisis/Reputation management
- Credit and identity monitoring services for those impacted by a breach
- Financial/Legal liability arising from those affected by the incident - customers, employees, vendors, and business partners, etc.

State of the Cyber Market

- Shift from commoditized privacy events to catastrophic ransomware events
- Ransomware events have more than doubled over the last few years
- Carriers have been forced into meaningful premium increases
- Significant reduction in overall capacity
- Starting to see some stabilization, but concern remains

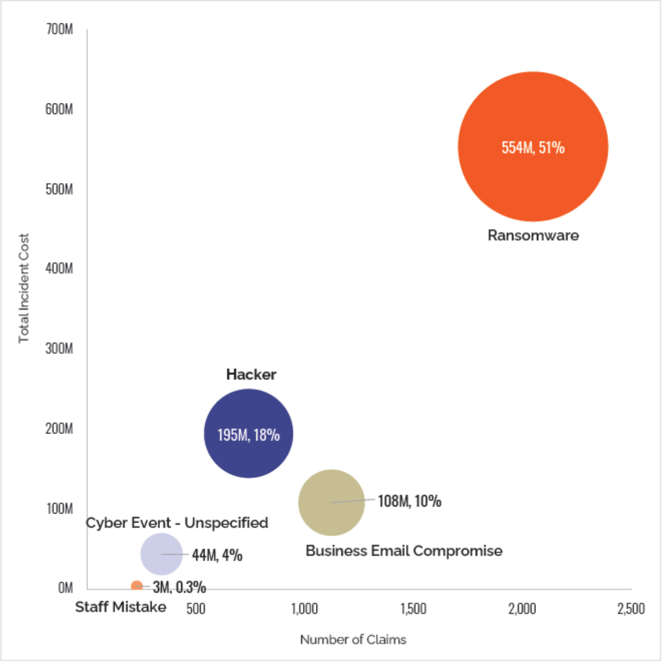
Loss Drivers & Trends

SMEs have become a major target

Top 3 Causes of Loss

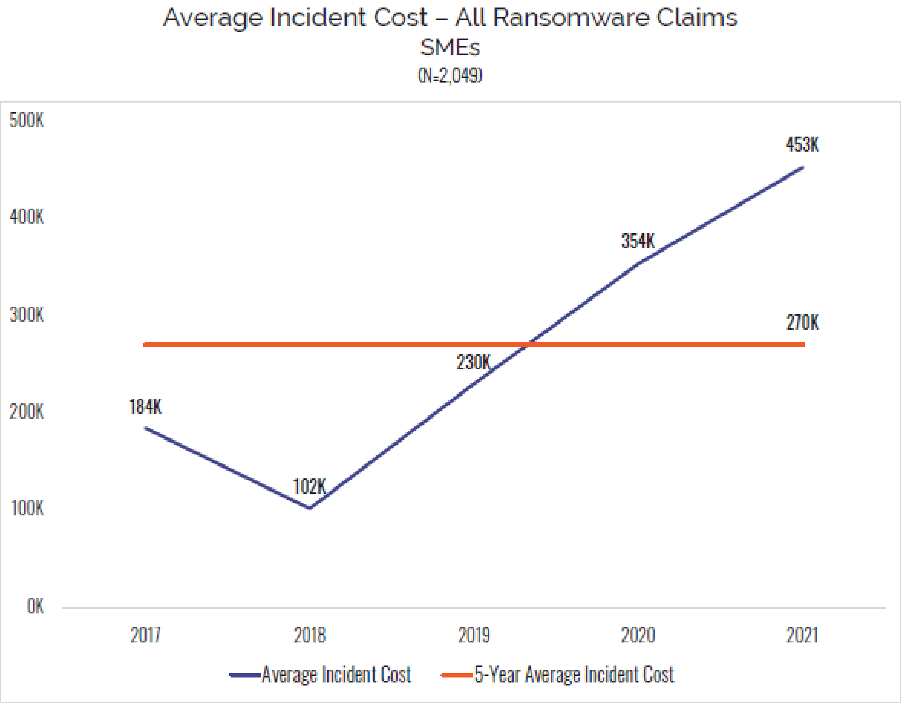
- Ransomware
- Business Email Compromise (BEC)
- Hacking/Data Privacy Event

Top Causes of Loss – SMEs
Number of Claims, Total Incident Cost, % of Total Incident Cost
(N=4,343)



**NetDiligence 2022 Cyber Claims Study*

Loss Drivers & Trends



**NetDiligence 2022 Cyber Claims Study*

Underwriting Process

- Process has become far more technical – significant changes for SME accounts
- Involve the right people in your organization
  - IT, HR, Finance, Privacy Officers, etc.
- Gather accurate data
  - Your technical staff or vendors need to be involved in the application process
- Be honest, don't guess!!!
  - Recent Travelers ruling
- Work with experienced insurance brokers

PHILADELPHIA INSURANCE COMPANIES
A Member of the Tokio Marine Group

ThinkPHLY

What Makes a Good Insured

Expected Cyber Controls

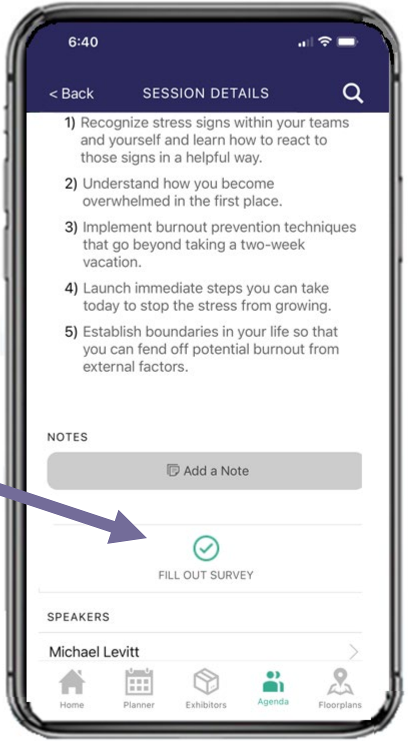
- Proper Email Security
- Multi-factor Authentication
- Air Gapped/Offline Segregated Backups
- Data Restoration Plan and Testing
- Business Continuity Plan
- Proper Patching Cadences
- Endpoint Detection and Response Systems

ANY
QUESTIONS
?

Use the App to Rate This Session!

- Log in to your profile
- Click “Agenda” on the app home screen
- Find the session
- Select “FILL OUT SURVEY”

Once you set up your profile, each session rating is an additional entry for one of five **$50 Amazon gift cards**!



1) Recognize stress signs within your teams and yourself and learn how to react to those signs in a helpful way.

2) Understand how you become overwhelmed in the first place.

3) Implement burnout prevention techniques that go beyond taking a two-week vacation.

4) Launch immediate steps you can take today to stop the stress from growing.

5) Establish boundaries in your life so that you can fend off potential burnout from external factors.

STAFFING WORLD® 2022