Creating a Cybersecurity Framework for PE Firms

EzeCastle
INTEGRATION

Today's Speakers

Mary Beth Hamilton
VP, Marketing
Eze Castle Integration

Bob Shaw
VP, Technical Architecture
Eze Castle Integration

Matthew Donahue
BCP & Cybersecurity Manager
Eze Castle Integration

Follow Along | @EzeCastleECI
#EzeCyber

EzeCastle
INTEGRATION

Agenda

- Introduction

- Today's threat landscape

- How to choose appropriate layers for your firm
  - Standard vs. Advanced

- Layers of Security

- Final Thoughts

- Questions

Microsoft
Tier 1 Cloud Service Provider

EzeCastle
INTEGRATION

Webinar Details

- The presentation is being recorded

- Full Survey Report will be provided post-webinar

- Follow along with us on Twitter!

Moving Targets: Today's Threats

Standard vs. Advanced Security Measures

We'll be covering Standard & Advanced elements throughout the discussion.

- ## Standard:
  - Security "must-haves"

- ## Advanced: ✚✔
  - Forward thinking IT solutions for institutional grade security

Asset Control & Management

- **Inventory and Control of Hardware Assets**
- **Inventory and Control of Software Assets**

Know What You Have

- **Secure Hardware and Software Configurations**
  - Deploy Standard Configurations
  - Manage/Enforce Configurations
  - Security Baselining Tools ✔

Technical Safeguards

- **Email and Browsing Protections**
  - Next-Generation Firewalls
  - Email Filtering & Anti-Phishing Service
  - Anti-Phishing Training Campaigns
  - DNS Level Filtering
  - Email Attachment Sandboxing

- **Malware Defenses**
  - Anti-Virus/Anti-Malware
  - Endpoint Protection
  - Malware Sandboxing & Detonation ✔
  - Anti-Exploit Technologies ✔

Network Security

- **Secure Network Device Configurations**
- **Boundary Defenses**
  - Encryption in Transit
  - Multi-factor Authentication
  - Next-Generation Firewalls
  - Network Intrusion Detection Systems ✔
- **Control of Network Ports, Protocols & Services**
- **Wireless Access Control**
  - Strong Authentication, Encryption, Firewalls, IDS, etc.
  - Segment Guest and Privileged Networks
  - Centralize Management

46% of employees access confidential information when using unsecure networks

Vulnerability Assessments & Pen Testing

- **Continuous Vulnerability Management**
  - Continuous External Vulnerability Scanning
  - Continuous Internal Vulnerability Scanning
- **Pen Testing and Red Team Exercises** ✓
- **Application Safety Software**
  - Code Review ✓
  - Vulnerability Testing ✓

Access Controls & Privileges

- **Controlled Use of Administrative Privileges**
  - Centralized Logging of Administrative Permission Use
  - Inventory of Privileged Accounts
  - Privileged Account Management

- **Need-to-Know Access Control**
  - Host-based Firewalls
  - Encryption in Transit
  - Implement Microsegmentation ✓
  - Data Loss Prevention ✓

- **Account Monitoring and Control**
  - Inventory/Document Accounts
  - Password Vaults
  - Disable Accounts in Timely Fashion
  - Centralize Account Management
  - Single Sign-on ✓

IT Resilience

- **Data Protection**
  - Data Inventory Systems
  - Endpoint Protection Systems
  - Whole Disk Encryption
  - Removable Media Restrictions
  - Data Classification Systems ✓

- **Data Recovery Capabilities**
  - Perform Regular Secure Encrypted Backups
  - Regularly Test Backup Integrity

Security Information and Event Management ✅

75% of SIEM adopters have seen reductions in their breach volumes and increased backend visibility

How SIEM Works

Collect and Aggregate Data From Multiple Sources

↓

Correlate Events via Statistical Correlation Engine that Identifies Relationships

↓

Identify Deviations and Take Action; Alert IT on Security Incidents

↓

Generate Real-Time Reports to Respond During Security Event

↓

Produce Post-Incident Forensic Reports to Remediate

Training Program & Incident Response

- Incident Response Program & Plan
  - Written Information Security Plan (WISP)
  - Incident Response Plan
  - Tabletop Exercises

- Security Awareness and Training Program Implementation
  - Security Awareness Training
  - Social Engineering/Anti-Phishing Training

70% of workers lack sufficient common data security knowledge

Final Thoughts

- There's no "one-size-fits-all" approach to cybersecurity

- There isn't one product, tool or technology to secure your assets

- For a free consultation on your cybersecurity strategy, please contact us at eci.com/contact

EzeCastle
INTEGRATION

Microsoft
Tier 1 Cloud Service Provider

Thank You

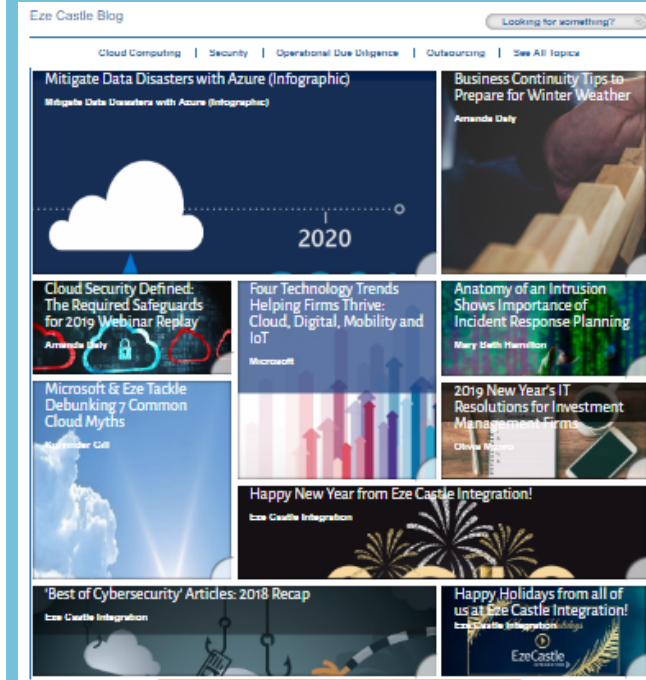**Mary Beth Hamilton**
VP, Marketing
Eze Castle Integration

Bob Shaw
Director, Technical Architecture
Eze Castle Integration

Matt Donahue
BCP & Cybersecurity Manager
Eze Castle Integration

Follow Along | @EzeCastleECI
#EzeCyber