Strategies to Avoid Common IT & Security Gaps

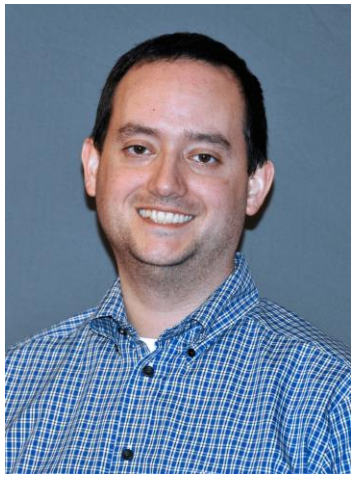
Follow Along

@EzeCastleECI
#CommonITGaps

EzeCastle INTEGRATION

Today's Speakers

Olivia Munro
Sr. Marketing Specialist
Eze Castle Integration



Steve Schoener
CTO
Eze Castle Integration

Alex Beher
Director of Service
Eze Castle Integration

Webinar Details

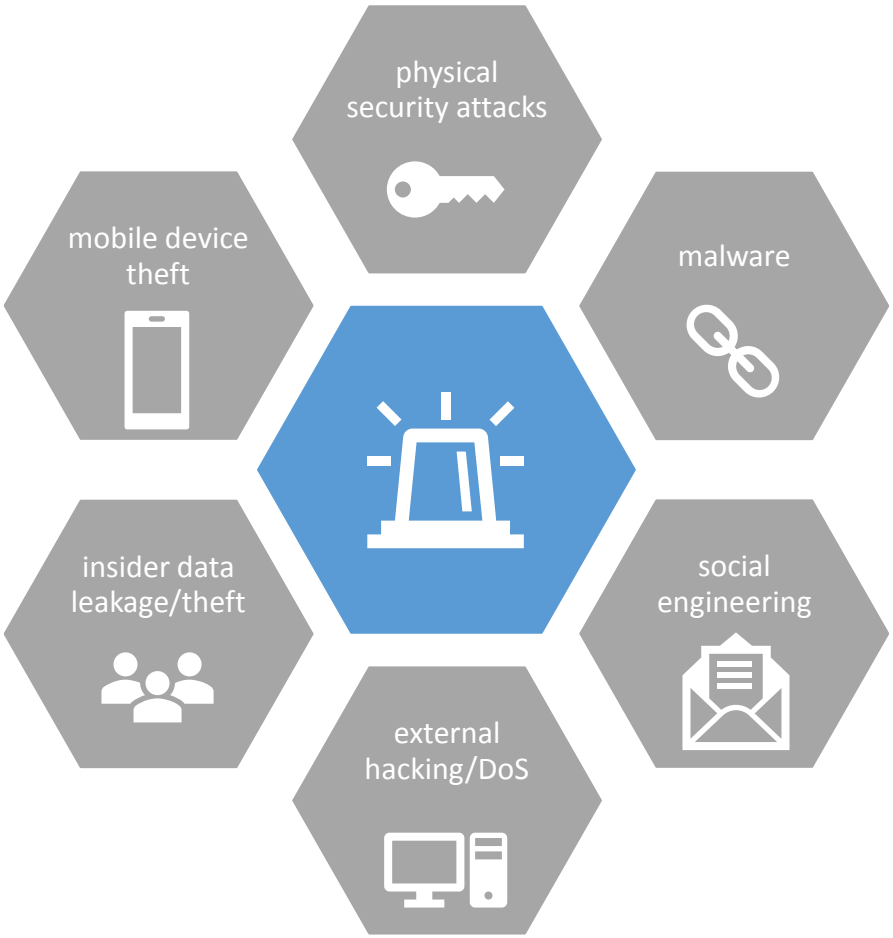
- Questions are welcome!

- Follow along with us on Twitter with #CommonITGaps

Today's Agenda

- Introduction
- Threat landscape
- Commonly overlooked IT & security gaps
- Easy fixes to IT holes
- Questions?

Moving Targets: Today's Threats



Governance, Oversight, Responsibility

Requirements can be from:

- Federal or international bodies or agencies
- State authorities
- Industry specific or even self-imposed by various groups or organizations

External pressures from:

- Investors
- Auditors
- External partners

IT Asset Management

- **Gap**: Firms don't have an inventory of all running IT Assets

- **Fix**: Keep a running list of all hardware and software, including:
  - Workstations
  - Servers
  - Applications
  - Smartphone devices such as phones, tablets and laptops

Patch Management

- **Gap**: Patches aren't tested/validated and applied appropriately or timely

- **Fix**: Automate patch management processes when possible
  - Test and validate patches first
  - Install patches as soon as they become available

Multi-Factor Authentication

- **Gap**: Firms aren't using multi-factor authentication (MFA)

- **Fix**: Enable MFA on all devices and applications:
  - Cloud platforms and remote access gateways
  - Social media sites
  - Web-based apps

User Provisioning & Management

- **Gap**: Access control policies aren't stringent enough or no policies are in place

- **Fix**: Instate the Principle of Least Privilege, leverage user provisioning software, have an official user provisioning posture in place

Vulnerability Assessments and Penetration Testing

- **Gap**: Failing to take a risk-based approach to cybersecurity

- **Fix**: Vulnerability assessments and pen tests, firms can identify real and potential risks that exist internal and external to the network

Social Engineering & User Training

- **Gap**: No formal employee cybersecurity training in place

- **Fix**: Commit to user education and training
  - Create a formal training program
  - General awareness help employees thwart any potential attacks

Business Continuity Planning

- **Gap**: The Firm has Business Continuity Plan in place, plan isn't communicated to employees, remediations aren't actionable

- **Fix**: Create an actionable, realistic BCP
  - BCP must be communicated to employees
  - Regularly update BCP
  - Ensure that the plan is actionable and realistic

Incident Response Planning

- **Gap**: Firm doesn't have an Incident Response Plan in place, or plan isn't thorough or realistic

- **Fix**: Have a realistic and actionable Incident Response Plan in place
  - Not if, but when, a security incident will occur
  - Culture of security comes from the top down

Third Party Vendor Management

- **Gap**: Firms have appropriate security measures in place, but don't monitor third party and vendor cybersecurity procedures

- **Fix**: Perform annual due diligence exercises with third party vendors and service providers

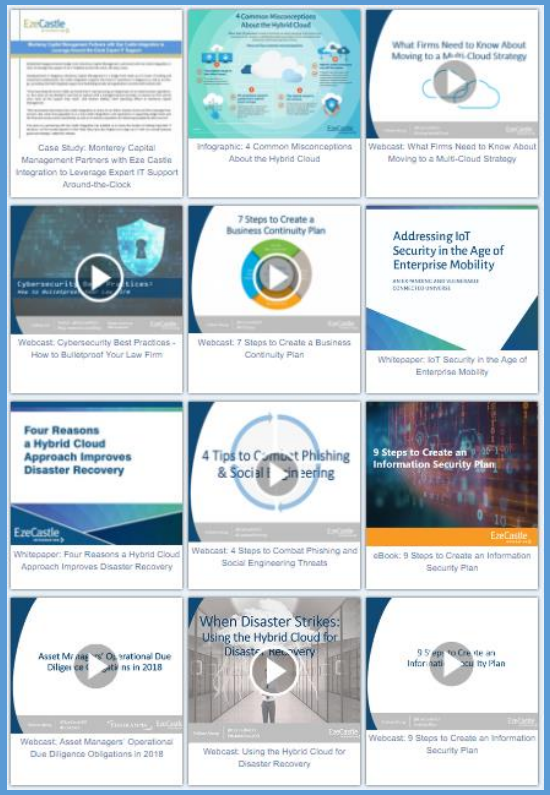
Questions?

Olivia Munro
Senior Marketing Specialist
Eze Castle Integration
omunro@eci.com

Steve Schoener
Chief Technology Officer
Eze Castle Integration
sschoener@eci.com

Alex Beher
Director of Service
Eze Castle Integration
abeher@eci.com

Thought Leadership



www.eci.com/resources

Follow Along | @EzeCastleECI #CommonITGaps

EzeCastle INTEGRATION