Welcome To The 10th Annual Hacking Conference
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!
Business Leadership and Cybersecurity Integration

- 10th Annual IIA/ISACA IT Hacking Conference
- Chicago, IL
- November 6, 2023

Eric Jeffery, TOGAF Master Architect
AlgoSec
Regional Solutions Engineer
eric.Jeffery@algosec.com
Agenda

• introduction
• leadership matters
• disparity requires variety
• true stories
• statistics
• engage and understand
• level up cyber security
• conclusion: solutions that make a difference
introduction
Disparate Entities Experience Unique Challenges
Distinct Enterprises Require Varying Solutions
true stories – beware & be aware
Third (4th, 5th, Etc.) Party Devastation

“The Biggest Hack of 2023 Keeps Getting Bigger” – Wired Magazine

Progress MOVEit

[Image of an explosion]
Major Brand Demolished

$100 Million

$100 Million
Children Impacted
bad guy statistics
Bad Guys are Everywhere and Have Completely Different Goals

WHO
- Nation states
- Organized crime
- Hacktivists
- Petty thieves
- Vandals
- Insider threats

WHAT
- Data theft
- Extortion
- Damage
- Embarrass
- Punish
- Signaling
- Shaping
- Coercion

https://threatmap.checkpoint.com
Cost of a Data Breach

Total cost of a data breach
USD 4.45M

- Global average total cost of a data breach

Time to identify and contain the breach

- 2023: 204 days, 73 days, 277 days
- 2022: 207 days, 70 days, 277 days
- 2021: 212 days, 75 days, 287 days
- 2020: 209 days, 73 days, 280 days
- 2019: 206 days, 73 days, 279 days
- 2018: 197 days, 69 days, 266 days
- 2017: 191 days, 66 days, 257 days

Type of data compromised

- USD 250,000
- 20% of organizations that experienced a data breach paid this much or more in fines

- USD 3.98M
- 51% of organizations increasing security investments after a breach

- 16%
- Percentage of breaches in which phishing was the initial attack vector

- 82%
- Share of breaches that involved data stored in cloud environments—public cloud, private cloud or across multiple environments

- 12%
- Share of data breaches originated from a software supply chain attack

- 33%
- Only one-third of breaches were identified by the organizations’ internal security teams and tools

- 2023
- United States: USD 9.48 million
- United States: USD 9.44 million
- Middle East: USD 6.07 million
- Middle East: USD 7.46 million
- Canada: USD 5.13 million
- Canada: USD 5.64 million
- Germany: USD 6.67 million
- United Kingdom: USD 5.06 million
- Japan: USD 4.52 million
- Germany: USD 4.86 million
engage and understand
Cyber Security Encompasses Everyone: The C-Suite Must Engage and Stay Involved
Understand Risk Management and Risk Quantification Inside the Enterprise

People, Property, Information

An **Asset** is what we’re trying to protect.

**Threat** – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. **A Threat is what we’re trying to protect against.**

**Vulnerability** – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. **A Vulnerability is a weakness or gap in our protection efforts.**

**Risk** – The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. **Risk is the intersection of assets, threats, and vulnerabilities.**
Is This a Risk or a Threat
This is a Threat
Countless Risks Exist in Cyber Security – How to Ensure Coverage

- Insider Threat
- Data Leakage
- Phishing
- Access Management
- Ransomware
- Worms
- Trojans
- Key Loggers
- Data Breach
- Version Control
- Third Parties
- Cloud Abuse
- Insecure Software
- Man In The Middle
- Patch Management

- Denial of Service
- Passwords
- Biometric Compromise
- Threat Vectors
- Network Penetration
- Lateral Movement
- Privilege Escalation
- Impersonation
- Social Engineering
- Shoulder Surfing
- Dumpster Diving
- Tailgating
- Shadow IT Systems
- Clear Text
level up cyber security throughout the organization
Who **Owns** What, Who **Does** What, Who **Knows** What

Governance = Leadership

- Engage
- Listen
- Decide
- Delegate
- Follow Up
- Track
- Shift as Necessary
- Reward
- Act and Keep Acting

<table>
<thead>
<tr>
<th>Relationship Manager</th>
<th>Vendor Manager</th>
<th>Project Manager</th>
<th>Account Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team Lead</td>
<td>Executives</td>
<td>Partner</td>
<td>Project Lead</td>
</tr>
</tbody>
</table>
Identify and Understand Those Responsible, Accountable, Supporting, Consulted and Informed (RASCI)

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision, install, and initially configure (IP address, connectivity, etc.) the SIEM SaaS System</td>
<td>R, A</td>
</tr>
<tr>
<td>Once able to remotely connect, take over the configuration of the SIEM SaaS System and customize it based on Client requirements, including Log Source integration, Use Case implementation, Dashboard customization, Offense Manager, and reporting</td>
<td>R, A C, I</td>
</tr>
<tr>
<td>Installation of licenses on the SIEM console</td>
<td>C, I</td>
</tr>
<tr>
<td>Installation of SIEM apps that require admin access to the SIEM console</td>
<td>R, A C, I</td>
</tr>
<tr>
<td>Allowing app access to specific user roles</td>
<td>R, A A, I</td>
</tr>
<tr>
<td>Installation of service token for apps</td>
<td>R, A C, I</td>
</tr>
<tr>
<td>Download, install, and configure all Client-premise Data Gateways and/or install physical Event Collector appliances and configure as Data Gateways.</td>
<td>R, A I</td>
</tr>
</tbody>
</table>

### Task Matrix

<table>
<thead>
<tr>
<th>Task</th>
<th>Vendor Management</th>
<th>Executive Sponsor</th>
<th>Business Owner</th>
<th>Legal</th>
<th>IT &amp; Info Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify standard terms &amp; conditions for contract</td>
<td>C</td>
<td>-</td>
<td>R/A</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Negotiate contract</td>
<td>C</td>
<td>C</td>
<td>R/A</td>
<td>C</td>
<td>-</td>
</tr>
<tr>
<td>Review final draft against standards</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R/A</td>
<td>C</td>
</tr>
<tr>
<td>Execute contract</td>
<td>I</td>
<td>R/A</td>
<td>C</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Store contract in contract management system</td>
<td>R/A</td>
<td>-</td>
<td>I</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Assign contract owner</td>
<td>R/A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Integrate new vendor through onboarding process</td>
<td>C</td>
<td>I</td>
<td>R/A</td>
<td>-</td>
<td>C</td>
</tr>
</tbody>
</table>
Understand Legal Requirements and Comply(ance)

California Consumer Protection Act (CCPA)
General Data Protection Regulation (GDPR)
Defense Federal Acquisition Regulation (DFARS)
Payment Card Industry Data Security Standard (PCI-DSS)
Health Insurance Portability and Accountability Act (HIPAA)

Sarbanes-Oxley (SOX)
Gramm-Leach-Biley Act (GLBA)

Federal Trade Commission Act §5
Children’s Online Privacy Protection Act (COPPA)
Standards and Frameworks to the Rescue in a Complex Arena

Just one mitigation breaks the chain

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies - 2024

ISO is an independent, international NGO with a membership of 165 national standards bodies. ISO has developed over 23400 International Standards.
conclusion: go forward with solutions that make a difference
Take a Giant Step Forward in the Cyber Security Journey
Businesses Must Understand Technology and NOT be Driven by Technology – Focus on the Problems at Hand

Mis-Aligned
Undigestible
Incomplete
Burn-out
Unnecessary

Overwhelming
Incompatible
Too Complex
Unmanageable
Redundant
Organization Wide, Organization Deep
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!
thank you