Cybersecurity Practices in Transportation & Logistics

Michael Ehrich
SVP of Global IT & Security
About Me

Michael Ehrich
SVP, Global IT & Security
project44
Chicago, IL
About project44

The world’s leading Advanced Visibility Platform™ for shippers and logistics service providers, project44 (p44) handles the data and analytics of a significant percentage of the global supply chain.

Headquartered in Chicago, IL

860+ Team Members across 25 countries

1,300+ Customers

240,000+ Carriers

1B+ Shipments Tracked Annually

10B+ Supply Chain Data Points per Month
NIST Cybersecurity Framework 2.0
National Institute of Standards and Technology (NIST)
Customers Trust project44

53 Security Controls

145 Security Controls
What’s a Security Control?

• A security control is a process, policy, or standard (safeguards or countermeasures) that mitigate risks and protect assets

• SOC and ISO controls are audited annually by their respective auditors

• project44 also performs an internal audit every six months on these controls

Types of Controls

• Process Controls (non-technical)

• Technical Controls
Examples of Process Controls

1. Penetration Testing
Examples of Process Controls

1. Penetration Testing

2. Security Awareness Training
Examples of Process Controls

1. Penetration Testing
   - DETECT

2. Security Awareness Training
   - PROTECT

3. 3rd Party / Vendor Risk Management
   - IDENTIFY
Product Security
Technical Controls
Examples of Technical Controls – Product Side

1. Encryption in Transit
2. Encryption at Rest
Examples of Technical Controls – Product Side

1. Encryption in Transit
2. Encryption at Rest
3. Multi-Tenancy Access Control
Examples of Technical Controls – Product Side

1. Encryption in Transit
2. Encryption at Rest
3. Multi-Tenancy Access Control
4. Web Application Firewall (WAF)
Web Application Firewall (WAF)
Examples of Technical Controls – Product Side

1. Encryption in Transit  PROTECT
2. Encryption at Rest  PROTECT
3. Multi-Tenancy Access Control  PROTECT
4. Web Application Firewall (WAF)  PROTECT
5. Multi-Region Replication  RECOVER
Examples of Technical Controls – Product Side

1. Encryption in Transit
2. Encryption at Rest
3. Multi-Tenancy Access Control
4. Web Application Firewall (WAF)
5. Multi-Region Replication
6. Backups & DR
Examples of Technical Controls – Product Side

1. Encryption in Transit
2. Encryption at Rest
3. Multi-Tenancy Access Control
4. Web Application Firewall (WAF)
5. Multi-Region Replication
6. Backups & DR
7. System Patching
Internal Security
Technical Controls
SaaS Design
Examples of Technical Controls - Internal

1. Unified Login (SSO)
With SSO

User → IdP

Applications:
- Microsoft
- Salesforce
- Zoom
- Zendesk
Without SSO
Examples of Technical Controls - Internal

1. Unified Login (SSO)  PROTECT

2. Multifactor Authentication (MFA)  PROTECT
Wells Fargo will NEVER call or text you for this code. DON'T share it. Enter Advanced Access code 365600 online to verify your identity.

Your E*TRADE verification code is 469269. No one from E*TRADE will contact you for this code unless initiated by you. Didn't request a code? Call 1-800-387-2331
MFA Rolling Codes
SSO with MFA

User → IdP → Applications

MFA

Logos © Microsoft, SAP, Salesforce, Zoom, and Zendesk
Icons © Microsoft

Copyright © project44 | Confidential
Passwordless Sign-in
FIDO2 Keys

Image © Yubico
Examples of Technical Controls - Internal

1. Unified Login (SSO)

2. Multifactor Authentication (MFA)

3. Trusted Devices
   a. Serial number match via Autopilot / ABM
   b. Enrolled and managed by project44 EDM (Endpoint Device Management)
   c. Full Disk Encryption
   d. Antivirus/Anti-Malware installed and updated
   e. Automated patching
   f. Other project44-specific policies / restrictions
Without Device Compliance

USERNAME → PASSWORD → MFA → SYSTEMS
With Device Compliance

USERNAME → PASSWORD → MFA → DEVICE → SYSTEMS
No Compliant Device?

USERNAME → PASSWORD → MFA → DEVICE → SYSTEMS
Monitoring

24x7 Incident Response

- Suspicious / unauthorized login attempts
  - Platform & Internal Systems
- Logins from suspicious IPs or locations
- Landspeed (impossible travel) violations
- Malicious URLs in emails
- Carrier outages

Threat intelligence from sources such as:
  - Microsoft, Crowdstrike, Cloudflare, and VirusTotal
Summary
# NIST Cybersecurity Best Practices

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Asset Management</td>
<td>• Security Awareness Training</td>
<td>• Penetration Testing</td>
<td>• System Patching</td>
<td>• Multi-Region Replication</td>
</tr>
<tr>
<td>• Vendor Risk Management</td>
<td>• Encryption in Transit</td>
<td>• SIEM</td>
<td>• 24x7 Incident Response</td>
<td>• Backups</td>
</tr>
<tr>
<td></td>
<td>• Encryption at Rest</td>
<td>• Monitoring</td>
<td></td>
<td>• Disaster Recovery</td>
</tr>
<tr>
<td></td>
<td>• Multi-Tenancy Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WAF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unified Login (SSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MFA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Trusted Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**GOVERN**

Policies, Processes, Procedures, Compliance (SOC 2 Type 2, ISO 27001)