Neutralizing Risk from Customer Engagements

Keely Richmond
Security Engineer, Check Point
MS Cybersecurity, Florida Institute of Technology

Email: krichmon@checkpoint.com
Twitter: @trulykeely
LinkedIn: https://www.linkedin.com/in/keely-richmond/
Outline

1. I am a Work In Progress
2. The Purpose of this Talk
3. Move or Rust
I am a Work In Progress

>25 years of honing my craft

**ROLES**
- Security Engineer
- Cybersecurity Manager
- Cybersecurity Consultant
- Network Security Engr/Team Lead
- Sr Ops & Sys Analyst
- Network Performance Engineer
- Network Management Analyst
- Data Warehouse Analyst
- Help Desk Technician

**INDUSTRIES**
- Security Vendor
- Value-Added Reseller (VAR)
- Tier 1 ISP / MSSP / International
- Finance
- Higher Ed & Medical
- Fortune 50 Enterprises

**EDUCATION**
- MS, Cybersecurity
- BS, Business Information Technology

**CERTIFICATIONS**
- GIAC GLEG
- Qualys (AV, VM, PC, +)
- ITILv3
- FireEye
- Palo Alto

Copyright © 2019 Keely Richmond
Disclaimer

This presentation is representative of my previous work experience. It does not reflect any work I have performed or witnessed with my current employer.

No company names are being used in the Case Studies; any uniquely identifying information that could be used to derive the company names has been anonymized.

Each of the companies referenced in this presentation either have or are in the process of rectifying the situations referenced in this presentation.
The Purpose of this Talk

Share some experiences that demonstrate how 3rd parties can inherit and transfer risk

Encourage action to neutralize those risks
Supply Chain Perspectives
<table>
<thead>
<tr>
<th>Term</th>
<th>Acronym</th>
<th>Description (as used)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan</td>
<td>BCP</td>
<td>Business plan defining the core requirements necessary to continue operation of the business</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>DRP</td>
<td>Business and/or technical plan defining how a business will recover from a disaster</td>
</tr>
<tr>
<td>Incident Response Plan</td>
<td>IRP</td>
<td>Business and technical plan defining how an organization will respond to a security incident</td>
</tr>
<tr>
<td>Service Provider</td>
<td>SP</td>
<td>Internet Service Provider and/or Telco</td>
</tr>
<tr>
<td>Subscriber</td>
<td>--</td>
<td>Residential or Business customer who uses the services provided by SP</td>
</tr>
<tr>
<td>Subscriber Network</td>
<td>--</td>
<td>Portion of the SP network used by subscribers for internet access</td>
</tr>
<tr>
<td>Operational Technology</td>
<td>OT</td>
<td>Technical team responsible for the availability and performance of an ICS or similar network; akin to the SP Engineering team within an SP org</td>
</tr>
<tr>
<td>Value Added Reseller</td>
<td>VAR</td>
<td>A company that contracts with vendors to sell product, but also provides value-added services ex. Implementations, assessments, etc.</td>
</tr>
</tbody>
</table>
Case Study Facts

Tier 2-4 Telco & ISP (regional & rural)

US Critical Infrastructure Communications Sector

Resource constrained (time, budget, staff)

No security regulatory or compliance requirements

“Inherited” networks with numerous 3rd parties in/out of network over years

Network availability prioritized over security
Two Case Studies

#1 The Eye-Opener

#2 Vendorgeddon
Case Study #1 Context

- The VAR is a network engineering company, not a dedicated security company.
- Details observed during Vulnerability Assessment performed by VAR.
- Assessment was designed from a Sales perspective – to sell specific tools.
- Various eye-opening discoveries found during Vulnerability Assessment.
- VAR tasked with operating within scope of contract i.e. discover & report.
Case Study #1: The Eye Opener

Typical Discoveries
- EoL/EoS equipment
- Grey market equipment
- Unsigned code
- Flat network & no redundancy
- Unpatched systems
- Configuration drift
- Inadequate network visibility
- Inadequate logging
- Inadequate 3rd party management
- Inadequate off-boarding of privileged users
- Inadequate access control mechanisms
- No BCP, DRP, IRP, etc.

Eye Openers 😳
- China & Russia IPs active on network
  - No attribution made; IPs can be spoofed.
  - Investigation is out of scope.
- Malware found on multiple systems
- >15K outbound files in approx. 24 hrs; some files identified as steganography
- Banned equipment (ex. Huawei)
- Forgotten devices found LIVE on the network
- Composition of subscriber-base (type & location of users) has far-reaching impacts

Copyright (c) 2019 Keely Richmond
Supply Chain Concerns

Malware
Nation-State Activity
Data Exfiltration
…and more

VAR IT & OT

Parent/Subsidiary

Employees

Vendors

Partners

3rd Parties

Customers
### Now What?

<table>
<thead>
<tr>
<th>CUSTOMER</th>
<th>3rd Party (VAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RECOMMENDED ACTION ITEMS</strong></td>
<td><strong>REASONABLE ACTION ITEMS</strong></td>
</tr>
<tr>
<td>Stop the bleeding</td>
<td>Scan equip used for assessment</td>
</tr>
<tr>
<td>Update BCP</td>
<td>Endpoint Security</td>
</tr>
<tr>
<td>Build actionable DRP &amp; IRP</td>
<td>VPN to Corp</td>
</tr>
<tr>
<td>Address Staffing/Skillset Issues</td>
<td>New VM per engagement</td>
</tr>
<tr>
<td>Full discovery of network</td>
<td>DLP</td>
</tr>
<tr>
<td>Align security strategy with BCP</td>
<td>Data Encryption</td>
</tr>
<tr>
<td>Operationalize security strategy</td>
<td>DNS</td>
</tr>
<tr>
<td>Vendor management</td>
<td>MFA</td>
</tr>
<tr>
<td>...and more</td>
<td></td>
</tr>
</tbody>
</table>

---

14

Copyright © 2019 Keely Richmond
• VAR is a network engineering company, not a dedicated security company

• VAR engaged to assist in configuring DDoS tool to help mitigate on-going attacks

• VAR further engaged to assist with root cause identification

• VAR further engaged to assist in mitigation and resolution efforts
Mayhem Afoot

- Sporadic equipment outages affecting subscriber internet access
- Time-based pattern of outages emerges
- In-house staff challenged to identify root cause
- Vendors and partners assist in troubleshooting
- No IRP, response is not well organized
- Situation persists ~2 months
- Millions of dollars lost to customer retention efforts, brand damage, battle-weary staff & vendors

Discoveries

- Unmanaged 3rd party with privileged access introduced malware, causing device & service outages
  - Determining intent is out of scope
- No process defined or actioned for managing vendors (on-boarding, off-boarding, oversight, audits)
- Composition of subscriber-base (type & location of users) has far-reaching economic impacts
Supply Chain Concerns

Malware
...and more!

VAR IT & OT

Parent/Subsidiary

Employees

Vendors

Partners

3rd Parties

Customers
Now What?

CUSTOMER

RECOMMENDED ACTION ITEMS

- Stop the bleeding
- Update BCP
- Build actionable DRP & IRP
- NEW Vulnerability Assessment
- Address Staffing/Skillset Issues
- Full discovery of network
- Align security strategy with BCP
- Operationalize security strategy
- Vendor management
- Penetration Testing

3rd Party (VAR)

REASONABLE ACTION ITEMS

- Scan equip used for engagement
- Endpoint Security
- VPN to Corp
- New VM per engagement
- DLP
- Data Encryption
- DNS
- MFA
- ...and more
There’s more!

**ACTIONS TAKEN**
Root cause = Malcode and suspect config introduced by vendor
Timeline & actions documented
Law enforcement engaged
Lawyers engaged
Insurance company engaged

**CHALLENGES**
Resources
Contention between objectives & priorities
Leadership Support

**LESSONS LEARNED**
• Competing objectives de-prioritize everything
• The cost of managing vendors is lower than the cost of unmanaged vendors
✓ Nothing about securing a business is easy.

✓ It **always** takes time, planning, funding, and commitment.

✓ Qualifying & quantifying the cost to prevent *something* can be enigmatic.

✓ Sometimes, doing nothing costs more than doing something.

✓ Planning & responding to risks should be proportional to the risk.

✓ Use a combo of contracts & technology to secure your interests.
Plan for Success & Sustainability

**STRATEGIC**
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Response Plan (IRP)
- + Other Policies

**TACTICAL**
- GRC
- Technical Solutions
- Business Management
- Design & Architecture
- Research & Development
- Business Development

**OPERATIONAL**
- Tools
- Processes & Procedures
- People
- Training
- 3rd Party Management
- Patch Management
- Config Management
- Access Controls
Risk Management

CHALLENGE
Awareness and mitigation of risk between entities

EFFECTIVE RISK MANAGEMENT
is the result of a deep understanding of the business and network,
regular pruning of the supporting policies & procedures,
and appropriate enforcement of each.

CAVEATS
• There is no One-Size-Fits-All Solution
• The ROI of risk management should be proportionate to the risk
What can we do about risk?

Understand (qualify & quantify) what is at risk.
Make choices based on what you know.

Accept

Avoid

Transfer

Mitigate
Neutralize the Risk

RULES OF ENGAGEMENT

• We *can’t dictate* how other organizations manage their business or perform their work.

• We can *control manage & monitor* access to our networks and systems, log their activity, and hold them to account for malicious or negligent activity.

• We can *utilize contracts* to encourage (or require) our supply chain partners to meet certain minimum standards of professional care, training, certification, audit, vulnerability assessment, penetration testing etc. and stipulate the financial impact of a breaching the contract.
Sample Controls

Contracts and Behaviors

• MSAs *(Master Service Agreements)*
• SOWs *(Statements/Scopes of Work)*
• Due Care and Due Diligence
• Audits, Vulnerability Assessments, Pen Tests
• Governance & Compliance (ex. ISO 27001, COBIT, PCI-DSS, NIST CSF)
• Professionalism, education, experience, certifications
• Escalations and points of contact
More Sample Controls

Access, Networks, and Systems

• Awareness

• Design & Architecture

• Visibility – network composition, content, and users

• Prevention – virus, malware, phishing, spear phishing, whaling, vishing, +

• Management – access, patching, configurations, users, signed code, encryption, EoL/EoS lifecycle, performance, business & technical rules

• Analysis – ingress/egress network traffic, anomalous activity

• Oversight – all privileged user activity, 3rd party activity, contract fulfillment
My “Normal” as a MSSP SOC Team Lead

Dedicated 3rd Party SOC/Threat Analytics team

Unmarked building (no corp branding)

Secured building, elevators, floor, room (cameras, badges, biometrics, guards)

VPN into customer network

Connect to VDI

No transfer of files between local system and VDI

Everything is monitored

ISO 27001 and ISO 9000 compliant
Move or Rust
Thank You