Cybersecurity Critical Path

How to Fast Track your Security Operations
About

- Matt Morton, CISM, CGEIT, CISSP

- Consultant, Vantage Technology Consulting Group
- CISO and experienced IT leader
Current State

- Survey Microsoft/Marsh
- NASCIO - #1 IT Issue 2015-2019
- CIO Magazine - #1 Issue for CIO’s 2019, 2018
  - Also top investment priority in same time period
- EDUCAUSE – Cybersecurity #1 IT Issue 2019-2016, 2008
- Society of Information Management Professionals (SIM) 2018 - Cyber at the top of survey results
Declining Confidence in Results
Microsoft/Marsh 2019

• 79% of respondents ranked cyber risk as a top five concern for their organization, up from 62% in 2017.
• Those saying they had “no confidence” increased:
• From 9% to 18% for understanding and assessing cyber risks.
• From 12% to 19% for preventing cyber threats.
• From 15% to 22% for responding to and recovering from cyber events.
Rising Incidents

• Two-thirds of cyberattacks affect businesses with fewer than 1000 employees
  • 2018 Verizon Data Breach Report

• The average cost of these cyber incidents is 1.43 million
  • Ponemon Institute 2018 State of Cybersecurity in SMBs 2018

• Only 17% of these businesses have a cybersecurity incident response plan
  • Better Business Bureau “State of Cybersecurity” Report 2017
## Annual Spend

<table>
<thead>
<tr>
<th>Market Segment</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>2,434</td>
<td>2,742</td>
<td>3,003</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>185</td>
<td>304</td>
<td>459</td>
</tr>
<tr>
<td>Data Security</td>
<td>2,563</td>
<td>3,063</td>
<td>3,524</td>
</tr>
<tr>
<td>Identity Access Management</td>
<td>8,823</td>
<td>9,768</td>
<td>10,578</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
<td>12,583</td>
<td>14,106</td>
<td>15,337</td>
</tr>
<tr>
<td>Integrated Risk Management</td>
<td>3,949</td>
<td>4,347</td>
<td>4,712</td>
</tr>
<tr>
<td>Network Security Equipment</td>
<td>10,911</td>
<td>12,427</td>
<td>13,321</td>
</tr>
<tr>
<td>Other Information Security Software</td>
<td>1,832</td>
<td>2,079</td>
<td>2,285</td>
</tr>
<tr>
<td>Security Services</td>
<td>52,315</td>
<td>58,920</td>
<td>64,237</td>
</tr>
<tr>
<td>Consumer Security Software</td>
<td>5,948</td>
<td>6,395</td>
<td>6,661</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>101,544</strong></td>
<td><strong>114,152</strong></td>
<td><strong>124,116</strong></td>
</tr>
</tbody>
</table>

In millions $USD

Source: Gartner (August 2018)
Security Program
Security Program

Technical Architecture
Simpler Way?

- Less complex
- More cost effective
- Easier to manage
- Easier to communicate
- Overall better results
Critical Path

- What is it?
  - The sequence of stages determining the minimum time needed for an operation, especially when analyzed on a computer for a large organization.

- Why is it useful?
  - Focuses efforts on important tasks in getting to desired results
Critical Path for Security

- Focus
  - What you own
- Identify
  - Assets
- Scan
  - Assets
- Review
  - Logs
  - Results
  - Accounts
- Secure
- Remove
  - Assets
  - Accounts
- Communicate
Focus

- Plan teams
- Review tools
- Setup ‘sprint’ standups
- Setup shared storage areas

- Setup time capture tools (spreadsheet)
- Identify and acknowledge areas that will not be perfect
- Identify the scope
- Clearly identify what you will NOT be doing!
- Set goals
  - # of assets, % scanned, % of accounts removed
Identify

- Review sources of asset information
  - Scans
  - Network scans
  - Purchase requisitions
  - Logs
- Compile asset list
- Classify assets
  - Criticality versus data stored/transmitted
- Start with those that have high criticality and high risk data
Scan

Scan . . .

- For vulnerabilities
- For high risk data (PII, etc.)
- With AV and Malware tools
- The network for activity
- Accounts
  - how are they used
- For shared credentials? (same login two IP’s maybe?)
Review

- Review all the results of scanning
- Spot check review logs of highest risk assets
- Spot check accounts with access to the highest risk assets
Secure

- Identify your border(s)
- Network IP ranges
- Cloud IP ranges
- If you have no firewall then plan for installation
- Review data in next sprint
- Verify firewall is protecting highest risk assets
  - Check rules
  - Test rules
Remove

- Assets/systems/endpoints not being used
- Question everything
  - “wait, what?”
- Remove data not being used
- Remove all access not being used
- Remove shared credentials
- Remove all deprecated accounts
Communicate

- What level of effort was expended?
  - In hours days or weeks
- What was accomplished?
- Use visuals if possible, to communicate outcomes
- Try to report progress weekly - simply
Critical Path Core Controls

- Asset Management
- Vulnerability Management
- Data Management
- Malware Management
- Secure Communications
- Access Control
- Log Monitoring
Asset Management

- Inventory Assets
  - Endpoints
  - Servers
- Applications (future)
- Cloud Services (future)

- Data
- Classify Assets
- Sources of data
- Scanning tools
- Purchase history
Vulnerability Management

- Consistent Scanning of all servers
  - Focus on exploitable vulnerabilities
  - Servers and desktops/laptops

- Automatic patching
  - Tuesday Updates
  - Turned on by default
Data Management

- Inventory data locations/flows
- Classify data by risk
  - High
  - Medium
  - Low
  - Public (maybe)
  - 3-4 levels
- Map data flows
  - Applications
  - Discover “hidden” data
  - Scan for PII
  - Backups
  - Test assumptions
Data Flow Mapping Example

Diagram:

- **SUPPLIERS**: Supplier 1, Supplier 2, Supplier 3
- **INPUTS**: Supplier 1 data element A, Supplier 1 data element B, Supplier 2 data element A, Supplier 2 data element B
- **PROCESS**: Step 1, Step 2, Step 3
- **OUTPUTS**: Step 1 data element A, Step 2, Step 3 data element A
- **CUSTOMERS**: Supplier 1, Supplier 2, Supplier 3

Diagram elements:
- Data Publisher (NGO)
- Data Publisher (Gov)
- Data Publisher (Funder)
- Data on Website
- External Data Source
- Aid Information Register (e.g., CKAN)
- Data Aggregator
- User
- External Service
- Data reformatted by user
- Process start
- Database
- Data inventory
- Made in Lucidchart
Malware Management

- Antivirus
  - Collect and review logs
  - How many infections are you getting?
  - How quickly is it being blocked/remediated?

- Malware Protection
  - Is there ransomware on your network?
  - Do you classify/analyze malware?
Secure Communications

- Protect the border
  - Border Firewalls
- Firewall/IDS on endpoints
  - Auto block
  - Review network communications from endpoints
- Email security
  - SPAM protection
  - Phishing Protection
  - Commercial works the best
  - DMARC
Access Management & Control

- Simplify Access
  - One Directory
- Protect high risk accounts
- Multi-factor
- Remove/Delete unused accounts
Log Review

- Consistent log review
- Start with something
  - 0% reviewed of 0 logs is still 0
- Identify key assets from inventory and begin with them
  - Is logging on?
  - Are the right fields being logged?
  - Can they be aggregated and reviewed?
Secret Sauce

- Agile project based
  - Rinse and repeat
  - Complete focus for 6 week sprints
  - Daily or weekly standups
- Identify knowns and unknowns upfront
- Identify measures to gauge progress
- Communicate the plan
- Have a party (with food)
Communicate

Sprint Results

- Assets: 297
- Logs: 29 GB
- Vulnerabilities: 1312
- Access: 393
- Malware: 47
- Communications: 23
- 15,345

Rating:
- Goal Met
- Partially Met
- Goal not Met

Effort:
- 7100 HRS
- 6.5 W

Assets:
- 569
- 123 Servers
Next Up

- Compliance (PCI, HIPAA etc.)
- BCP
- Wireless
- Mobile
- Application Security
- Cloud Security
- Risk Management
- Physical Security
- Data Governance
- Operational System Security
- IoT
Questions?
Tools
Asset Management Tool Example

- https://snipeitapp.com/demo
Patching

Install and Update All Your Programs at Once
No toolbars. No clicking next. Just pick your apps and go.

Ninite

- Installing Dropbox...
- Chrome: Skipped (up to date)
- Skype: OK
- Spotify: OK
- Dropbox: Installing
- LibreOffice: Downloading
- Malwarebytes: Waiting to download
Vulnerability Management

Example

Open VAS

http://openvas.org/
Data Discovery

Open Source
- SENF - https://github.com/utiso/senf
- ccsrch - https://sourceforge.net/projects/ccsrch/
- Open DLP - https://code.google.com/archive/p/opendlp/
- Gliffy
- LibreDraw

Commercial
- Spirion
- Symantec
- SolarWinds
AV & Malware Tools

- MS Windows Defender
- Clam AV (Clam WIN) - https://www.clamav.net/
- Immunet (CISCO Amp) - https://www.immunet.com/index
- AVG*
- Panda*
- Bitdefender*
- Research test results - https://www.av-comparatives.org/

* Free is not free – your data is the product
Cuckoo Sandbox
Secure Communications

- Glasswire ($) - https://www.glasswire.com/
- pfSense - https://www.pfsense.org/
- ClearOS - https://www.clearos.com/
- Smoothwall - http://www.smoothwall.org/
- VyOS - https://vyos.io/
- DMARC
  - Fraudmarc CE - https://www.fraudmarc.com/fraudmarc-ce-open-source-dmarc/
  - DMARC.org
  - Trusted Domain Project - http://www.trusteddomain.org/opendmarc/
Glasswire
pfSense
ClearOS

Network Report - Interface - eth0

The Network Report provides network throughput information on all your network interfaces.

Report Data

<table>
<thead>
<tr>
<th>Date</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-12-01</td>
<td>600</td>
<td>675</td>
</tr>
</tbody>
</table>

Home Reports

Welcome to the Home Reports!
These reports are designed to be useful in home environments.

Filter:

- Date Range: Today

Reports:
- Overview
- Interface - eth0
Smoothwall
Access Management Tools (open)

- gluu Identity Server
- Oxpush (multifactor)
- Azure Active Directory
Log Tools

- Kafka - [https://kafka.apache.org/](https://kafka.apache.org/)
- Jupyter- [https://jupyter.org/](https://jupyter.org/)
- Graylog
- Elastic Stack (ELK)
- syslog
In Depth: Linear Regression

Just as Naive Bayes (discussed earlier in In Depth: Naive Bayes Classification) is a good starting point for classification tasks, linear regression models are a good starting point for regression tasks. Such models are simple because they can be fit very quickly, and are very interpretable. You could probably load up the simplest form of a linear regression model (i.e., fitting a straight line to data) but such models can be extended to model more complicated data behaviors.

In this section we will start with a quick recipe walk-through of the mathematics behind this well-known problem, before seeing how to approach it to see how linear models can be generalized to account for more complicated patterns in data.
## Example

<table>
<thead>
<tr>
<th>TASK</th>
<th>PROGRESS</th>
<th>START</th>
<th>END</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify ITS Servers &amp; WebApps</td>
<td>100%</td>
<td>4/9/18</td>
<td>5/11/18</td>
</tr>
<tr>
<td>Develop Data Standards, Training, and User Guide for Asset Library</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Library data quality management</td>
<td>25%</td>
<td>4/9/18</td>
<td>5/10/18</td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and assign risk to ITS web sites</td>
<td>90%</td>
<td>4/9/18</td>
<td>5/11/18</td>
</tr>
<tr>
<td>Perform web app scans of high risk assets</td>
<td>25%</td>
<td>4/9/18</td>
<td>8/20/18</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify high impact vulnerabilities - Project Adobe</td>
<td>100%</td>
<td>4/9/18</td>
<td>5/12/18</td>
</tr>
<tr>
<td>Identify high impact vulnerabilities - Project Java</td>
<td>25%</td>
<td>5/7/18</td>
<td>6/15/18</td>
</tr>
<tr>
<td>Identify and add ITS servers into the Vulnerability Management scanning process</td>
<td>31%</td>
<td>4/9/18</td>
<td>10/11/18</td>
</tr>
<tr>
<td>Network Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify key edge protection points for ITS assets</td>
<td>90%</td>
<td>4/9/18</td>
<td>6/1/18</td>
</tr>
<tr>
<td>Web Application Firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify ITS web apps that need to go behind the I3</td>
<td>75%</td>
<td>4/23/18</td>
<td>6/1/18</td>
</tr>
<tr>
<td>Build framework and train personnel</td>
<td>25%</td>
<td>4/23/18</td>
<td>8/7/18</td>
</tr>
<tr>
<td>Authentication and Provisioning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and standardize ITS services’ authentication process</td>
<td>10%</td>
<td>5/14/18</td>
<td>7/15/18</td>
</tr>
<tr>
<td>Logging and SEM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build consolidated framework</td>
<td>50%</td>
<td>4/9/18</td>
<td>7/1/18</td>
</tr>
<tr>
<td>Investigate new solutions for log retention</td>
<td>50%</td>
<td>4/9/18</td>
<td>6/23/18</td>
</tr>
<tr>
<td>Identify and remediate systems not sending log</td>
<td>25%</td>
<td>4/9/18</td>
<td>10/22/18</td>
</tr>
<tr>
<td>Identify correct logs are being ingested</td>
<td>40%</td>
<td>4/9/18</td>
<td>8/10/18</td>
</tr>
</tbody>
</table>
• A seventeen year old Technology Consulting Firm with offices in New York, Boston, Los Angeles and San Francisco.
• We have a forward looking vision coupled with an attention to detail.
• We look for opportunities for integration between technologies, systems and applications.
• We avoid “technology for technology’s sake” by looking for value in the systems we design.
• We speak the language of our clients to match expectations with project deliverables.
VANTAGE TECHNOLOGY SERVICES

- Strategic Technology Planning
- Business Continuity / Disaster Recovery Planning
- Operational and Organizational Planning
- Infrastructure Design and Engineering
- System Design and Specification
- Bid and Procurement Management
- Construction Administration
- Implementation Project Management
- Transition Planning and Activation Assistance