Security Technology Portfolio Management

Jim Routh
CSO
Aetna
Session Objectives

1. **Encourage you to take more risks in order to manage risk more effectively**

2. **Share techniques for managing security technology portfolio risk**

3. **Identify methods for applying innovation to the evolution of control design to change the rules for threat adversaries**
A Chief Information Security Officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks.
The existing rules favor adversaries

1. Victim clicks on an URL in a phishing email

2. Threat actor uses access to gain privilege

3. TA uses privilege to exfiltrate and monetize data
Conventional controls are good and insufficient

**NIST Cybersecurity Framework**
- NIST 800-53
- PCI-DSS 3.0
- Shared Assessments SIG
- Shared Assessments AUP
- SOC 1 & 2
- BSIMM

**UNCONVENTIONAL**

**CORE**
- Vulnerability Management
- Software Security Program
- Mobile Security Program
- Identity & Access Management
- Security Data Analytics
- Adaptive Enablement (DLP)
- BYOD Controls
- Federated Identity Management
- Cloud Security Controls
- Cyber Threat Intelligence
- Policy Management (eGRC)
- Education & Communication
- Security Steering Committee
- Threat, Vulnerability Assessment
- Asset Inventory Prioritized by Risk
- Information Classification Policy
- Configuration Management
- 3rd Party Governance
- Incident Response
- Behavioral Based Authentication

**Top Key Control Test Results**
- BitSight Vulnerability Review
- Security Scorecard Vulnerability Review
- Synack Pen Test Results (crowdsourced)
- Email Sinkhole
- DMARC
- Domain attribute filtering
- PUM and PAM
- Next generation authentication
Innovation comes from entrepreneurial firms
Technology Portfolio

Investment Philosophy

65% Legacy Technology
- Mature
- Meets basic requirements
- Established companies
- Financially sound
- Enterprise scalable

10% Replacement of Legacy
- Needs upgrade
- No longer mitigates risk

25% New Acquisition
Portfolio Management

Angel/Early Stage

Product/Service

The Norm

Investment Opportunity

VC Backed

Round 1

Round 2

Round 3

IPO

Private Equity

Market Share

Price

The Norm
Procurement Criteria

**Conventional**
1. Market share
2. Enterprise scalability
3. Enterprise customer feedback
4. Financial resiliency
5. Liability insurance level
6. Industry knowledge
7. Demonstrated track record

Volume discount off list price

**Unconventional**
1. Game-changing capabilities
2. Founder’s ability to attract engineering talent
3. Adult supervision - business acumen
4. Engineering team’s ability to pivot
5. Ability to listen to enterprise client requirements

Very low acquisition price

Risk mitigation
Vendor Prospect List
1. Vendor A
2. Vendor B
3. Vendor C...

Conventional

Financial Resiliency

Competitor Analysis

International Scalability
Revised Procurement Process

Valley Visits Agreement

• Identify trends, categories, early stage companies
• Game-changers

Mutual Non-Disclosure Agreement

• Protects both firms
• Facilitates IP sharing

STEEP Session

• Security Technology Exploratory Evaluation Process
• 20-60 participants
• Education on emerging capabilities
• No sales people, no selling
• Problem statement and the architecture
• Technical depth

SCARF

• License agreement for a POC Project
• Enterprise Architecture formally engaged

90 Day POC

• Proof of Concept Project with iterative testing
1. Container technology enables the acceleration of a DevOps model for the large enterprise

2. Network architecture is changing at its core- Switch replaces a NIC card

3. To attract technical talent in the valley...go into residential real estate
Example of IT Trend 2015

1. Smart switches connect directly to the server
2. Switch uses PCIe interface at the kernel level
3. Network traffic can be shaped with more ports increasing throughput

How will this influence compute architecture and ultimately security?
2015 Categories of Interest

1. Software defined networking
2. Cloud security- SAS and PAS
3. DevOps Security
2013 Shopping List

• Network behavioral analysis (NBA)-
• Data loss prevention (DLP)-
• Cloud service consumption or dark network controls
• Intrusion detection services (IDS)
• Machine learning applied to entitlement data
• Privilege user monitoring (PUM)
• Mobile risk scoring engine
• Fraud detection and management capabilities
• Host based intrusion detection
• B2B Connection behavioral monitoring
• Software security program components
Layered Controls

Host-based intrusion detection 1
Market leader

Host-based intrusion detection 2

White listing processes

Micro-virtualization
Botnet Filtering

Aetna Customers

Attackers/Content Scrapers

Automated traffic can no longer send valid requests

Legitimate traffic encounters no barriers
More Un-Conventional Controls

According to the 2015 Verizon Data Breach Investigations Report (VDBIR):

- Phishing was associated with 95% of incidents attributed to state-sponsored threat actors
- Over 100 million phishing messages arrive in our inboxes every day
- The median time-to-first-click came in at one minute and 22 seconds across all campaigns

What can we do?

- Improve education/awareness
- Consider designing new controls

23% of recipients now open phishing messages and 11% click on attachments

Nearly 50% open emails and click on phishing links within the first hour

1. Implement DMARC for all outbound email
2. Upgrade email gateway payload inspection and filters
3. Sinkhole all new domains for 48 hours
4. Enforce inbound filtering (DMARC)
DMARC for Outbound Mail

Trusted email delivers:

1. Reduced risk to consumers
2. Lower operating costs from the elimination of account takeovers
3. Higher profit from an increase in email click-through rate
A sinkhole, also known as a cenote, sink, sink-hole, shakehole, swallow hole, or doline (the different terms for sinkholes are often used interchangeably), is a depression or hole in the ground caused by some form of collapse of the surface layer.
Using email traffic data, the system learns the **unique fingerprint** of all email senders into your enterprise.

29,231 servers sent email for an enterprise on a single day.

This durable **identity trust model** is used to stop all messages that do not prove they should be trusted.

- **312** servers for the enterprise
- **4,641** servers owned by service providers
- **9,732** benign email forwarders
- **14,526** malicious senders
Privilege User Monitoring

1. Reduce the number of privilege users

2. Provide context to monitoring

3. Implement data analytic techniques to determine behavioral patterns