SECURBORATION

Cyber Security Issues

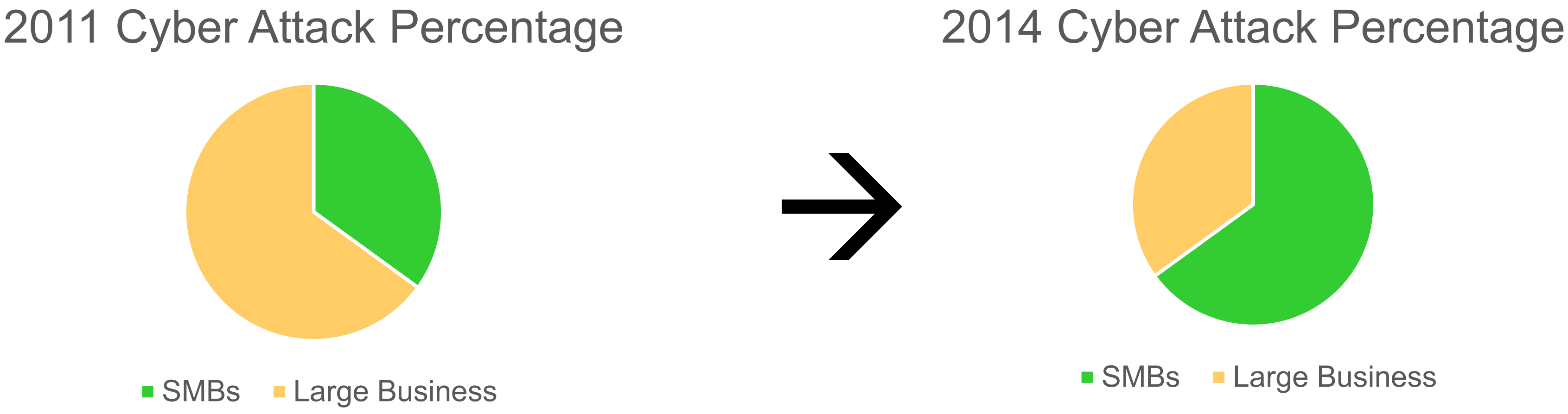
Overview

- Cyber Growing Problem for SMBs
- Understanding the Attacker
- Addressing the Cyber Problem
- Summary / Q&A

Cyber is a Growing Problem for SMBs

Cyber Attacks Favoring SMBs

- Cyber attacks targeting SMBs have grown from less than 40% in 2011 to over 60% in 2014 (Symantec Security Threat Report and Verizon Data Breach Report)
- Target data breach was initiated by a small business owner clicking a link in a phishing attack
  - His compromised credentials to the Target portal for suppliers led to the installation of bots that found unencrypted PII on backend systems and unencrypted PCI on PoS devices



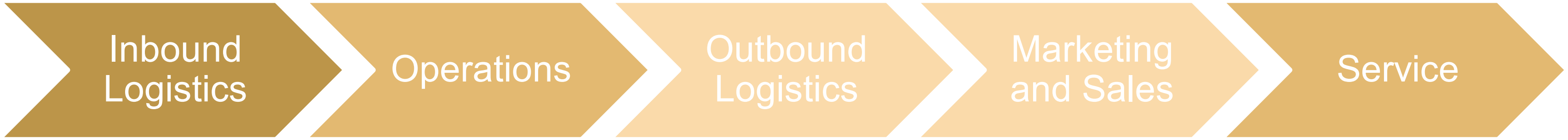
2011 Cyber Attack Percentage

2014 Cyber Attack Percentage

SMBs provide faster success than layered defense-in-depth found at many large businesses

Cyber is a Growing Problem for SMBs

Hacker Perspective of SMB



Inbound Logistics

- Suppliers
- Handling materials
- Warehouse
- Inventory management

Operations

- Conversion
- Assembly
- Packaging
- Maintenance

Outbound Logistics

- Warehouse
- Order fulfillment
- Shipment
- Delivery

Marketing and Sales

- Channels
- Product, pricing, promotion, distribution
- Business development
- Salesforce

Service

- Installation
- Repair
- Training

Procurement	Technical Development	Human Resources	Infrastructure
Requirements Purchasing Vendor management Fixed assets	Process design Product design R & D Sunsetting	Talent acquisition Training Succession planning Compensation, benefits	General management Finance Accounting IT

Cyber is a Growing Problem for SMBs

Most SMBs Are Not Prepared to Battle Cyber Attacks

- More than 40% of SMBs do not have adequate IT security budget (Ponemon Institute Nov 2013)
  - Are considered easier prey by well-funded hacker groups targeting a larger business network
    - Source:Federal Bureau of Investigation
- 77% of SMBs believe their company is safe from cyber attacks
  - Source: National Cyber Security Alliance
- National Small Business Association survey found that almost half of SMBs have the business owner or no one specific handle IT security
  - Approx. 1/4th of the SMBs had an IT security expert involved in their IT system

SMBs need a low-cost, easy-to-deploy, secure compute environment that provides layered defense-in-depth

Cyber is a Growing Problem for SMBs

Common Reasons for Lack of Cyber Security

- Lack of cyber security policy
- Lack of time, budget and expertise to enforce cyber security policy and implement comprehensive security defenses
- No dedicated IT security specialist on the payroll
- Outsourcing security to unqualified contractors or system administrators
- Lack of cyber security and risk awareness
- Lack of employee training on cyber threats and vulnerabilities
- Failure to regularly update security controls
- Failure to secure endpoints
- Not needed, because data is not of great value

Small businesses with revenues less than $100M cut security spending by 20% in 2014,
while large businesses increased their cyber spending by 5%
PWC's Global State of Information Security Survey 2015

Cyber is a Growing Problem for SMBs

SMB Cyber Equation

Easier Target

+

Lack of Skills and Tools

=

Very Bad Ending

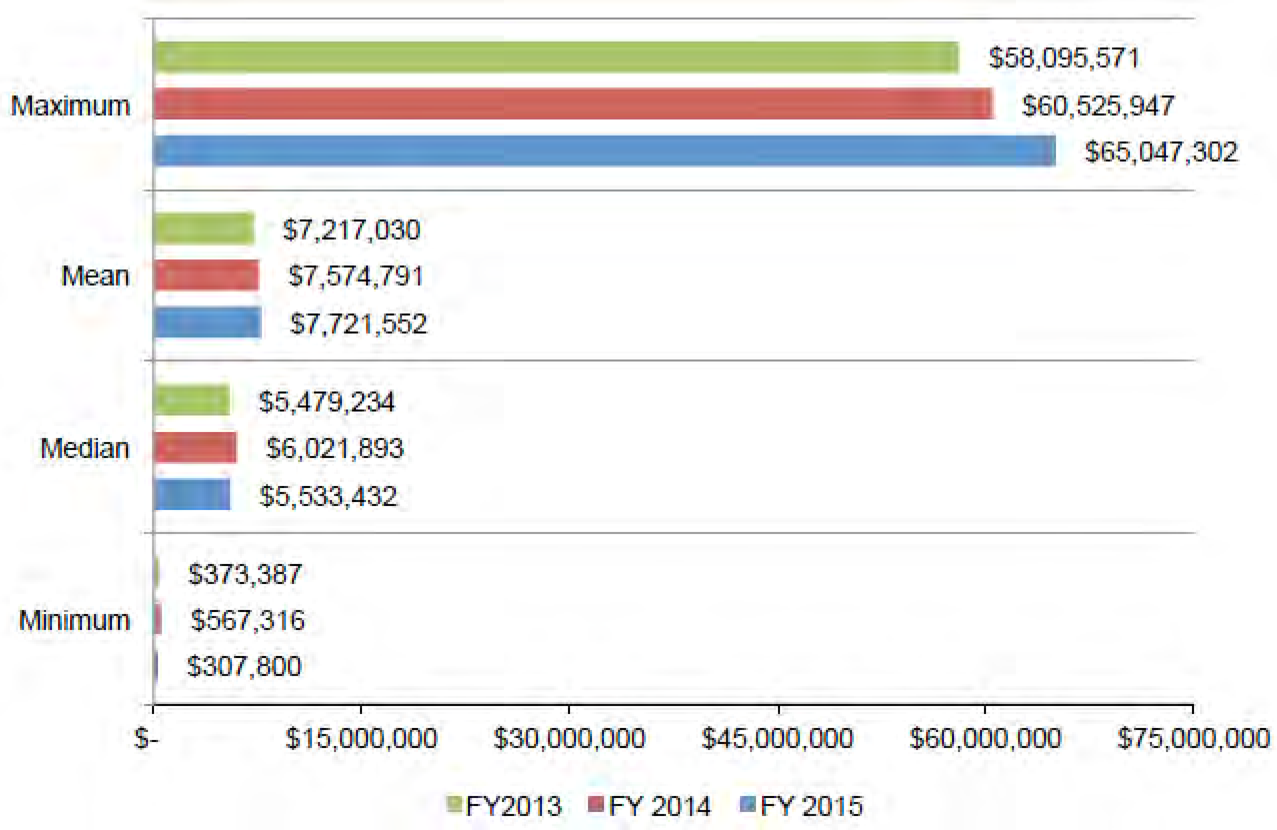
Cyber is a Growing Problem for SMBs

Cyber Attack Effects on SMBs

- 60% of SMBs close doors within six months of a data breach
  - Source: National Cyber Security Alliance
- Loss of Intellectual Property
  - Competition
  - Costs
- Loss of Contract for Third-Party Data Loss
- Litigation and Legal Expenses

Cyber is a Growing Problem for SMBs

Cyber Attack Costs



Source: Ponemon Institute Global Cost of Cyber Crime Report for 2015

Understanding the Attacker

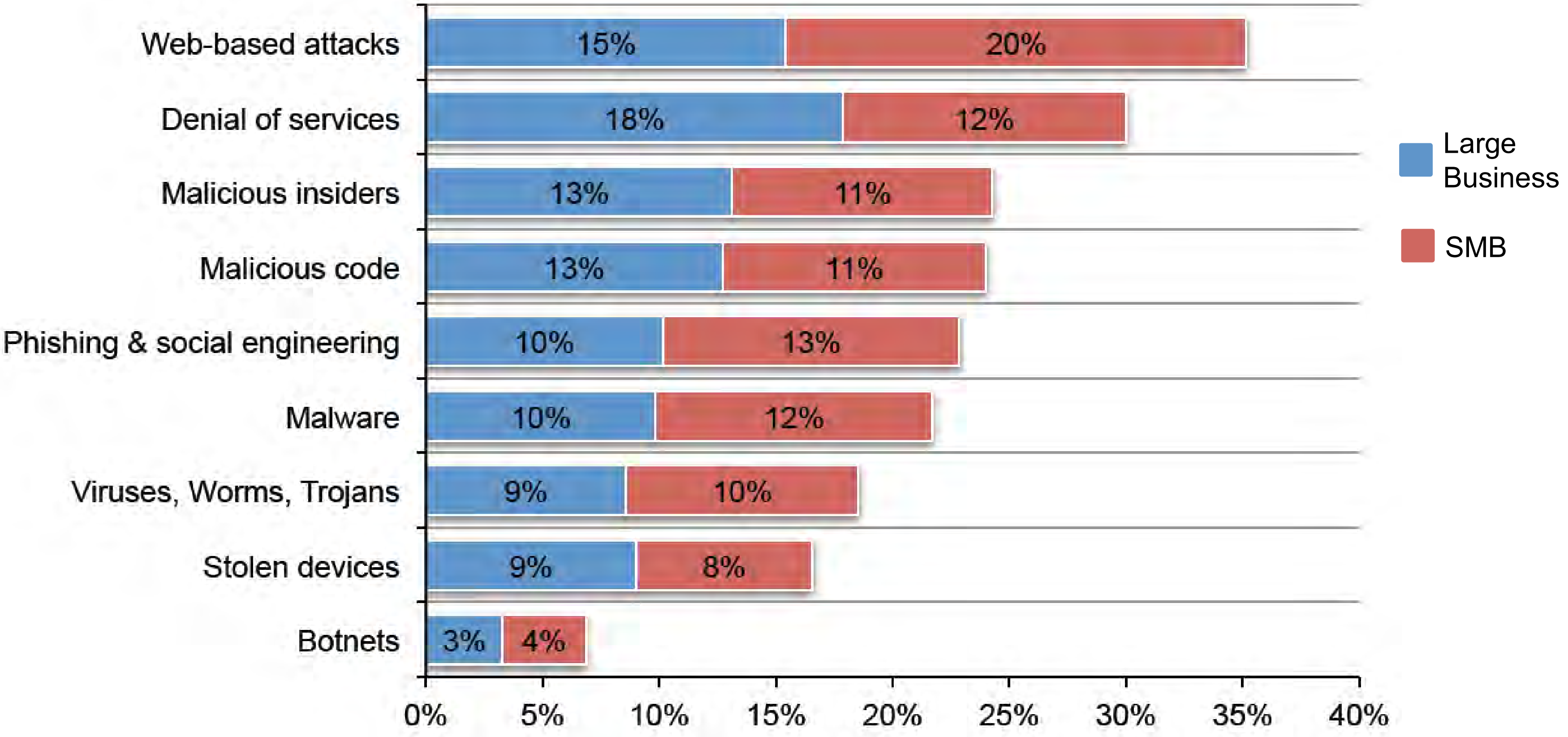
Common Attack Vectors

- Employee and Affiliate Misuse
- Phishing
- Malware
- SQL Injection
- Cross-Site Scripting
- Brute Force Password Cracking
- Denial of Service
- Social Engineering Man-in-the-Middle
- Device Theft

SECURBORATION

Understanding the Attacker

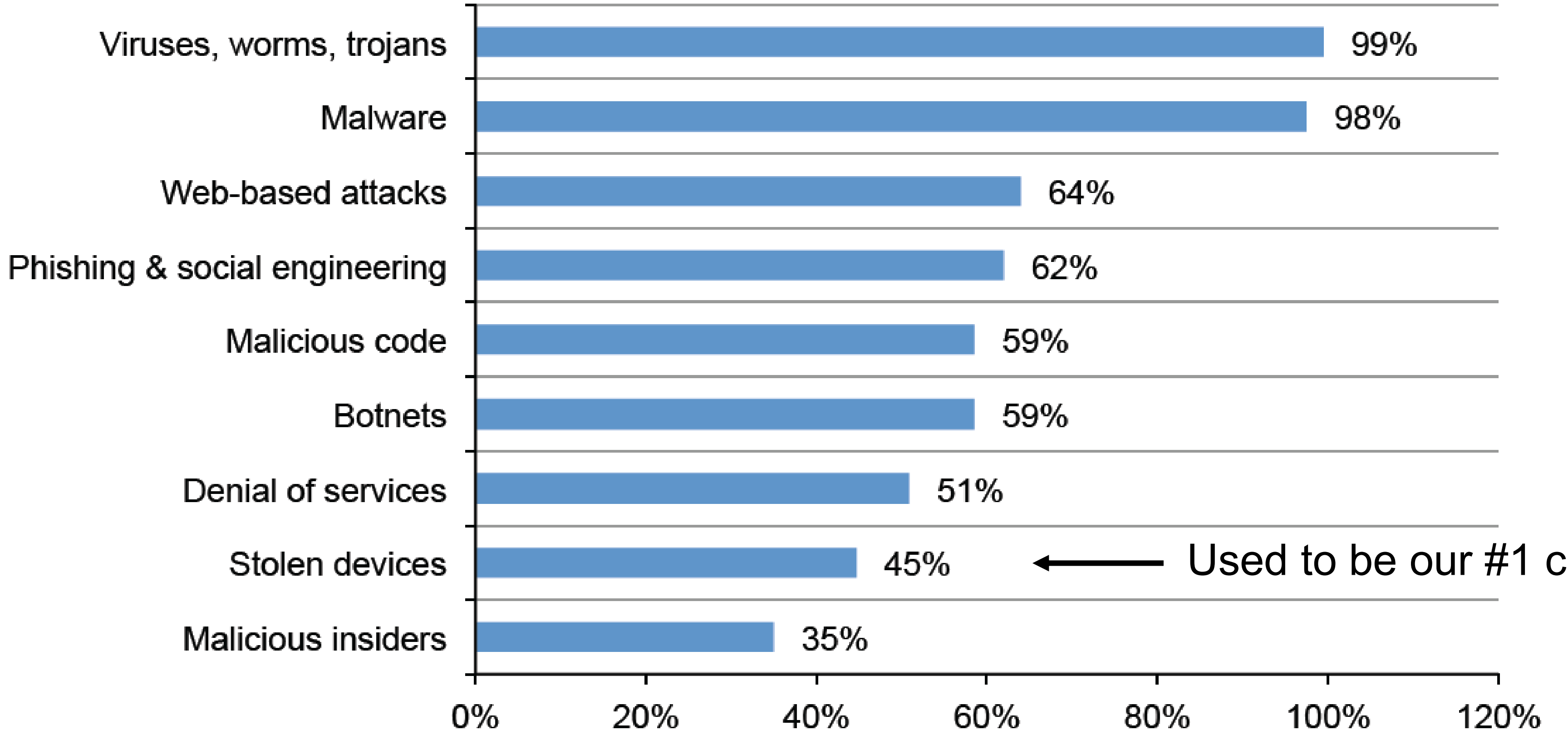
Common Attack Vectors



Source: Ponemon Institute Global Cost of Cyber Crime Report for 2015

Understanding the Attacker

Common Attack Vectors



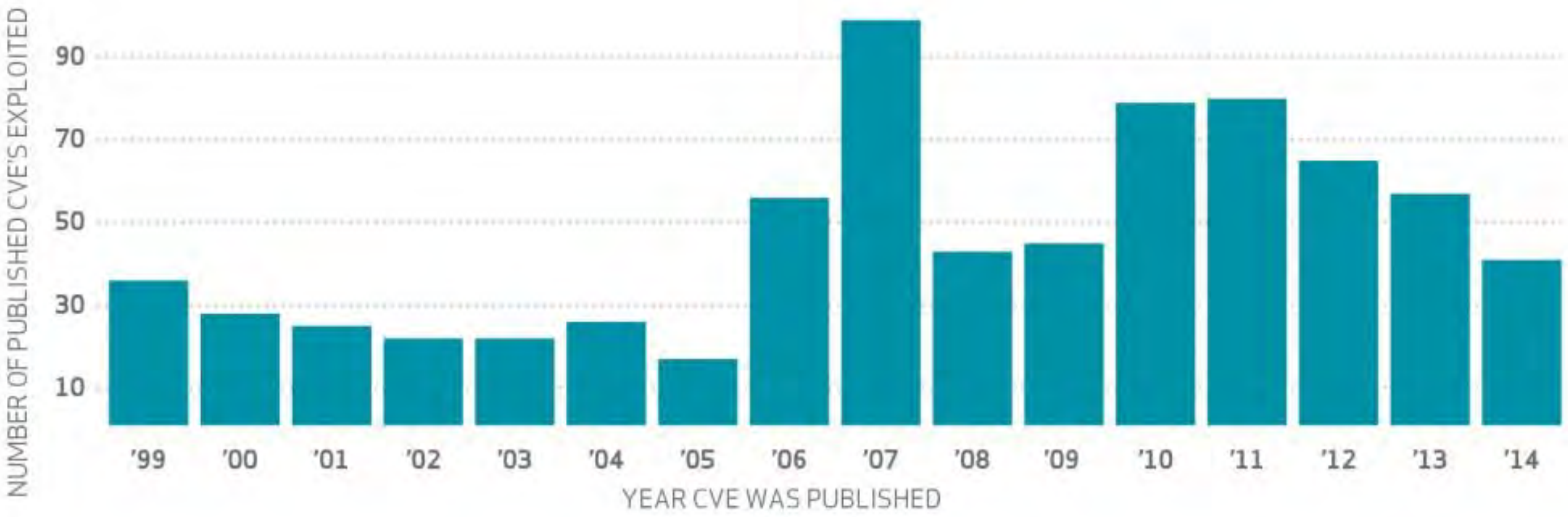
← Used to be our #1 concern

Source: Ponemon Institute Global Cost of Cyber Crime Report for 2015

Understanding the Attacker

Attack Methods by Age of Attack Method

- 95% of data breaches investigated by Verizon from 2014 were caused by Common Vulnerabilities and Exposures (CVE) issues over a year before the exploit
- 97.7% of all breaches were from 10 CVEs



Source: Verizon Data Breach Investigations Report 2015
http://www.verizonenterprise.com/DBIR/2015/

Understanding the Attacker

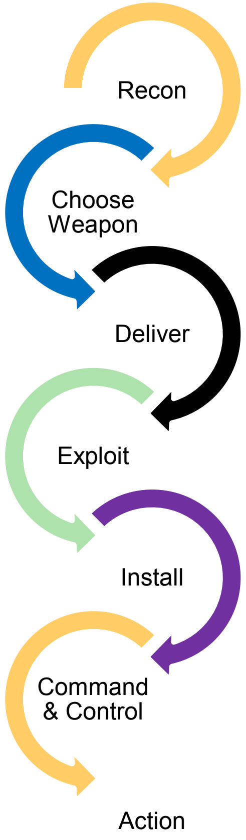
Types of Cyber Attacks

- Non-invasive: Using cyber assets to damage an entity without entering the entity's cyber domain
  - Cyber bullying is one example
- Indiscriminate: Damaging cyber, and potentially non-cyber, domain(s) of an entity with no discriminating intent to damage one or more specific entity(ies)
- Targeted: Intent to damage cyber, and potentially non-cyber, domain(s) of a specific entity or group of entities
  - Ad Hoc: Hacking activities "on-the-fly", often in a single sitting … commonly referred to as "the 8-minute hacker"
  - APT: Advanced, Persistent Threat that may take months to recon a target before delivering specific agent(s) designed to exploit specific vulnerability(ies)
  - Cyber Warfare: Nation state and/or crime group sponsored attacks that typically used multiple APT and Ad Hoc attacks simultaneously

Understanding the Attacker

Attack Methodology / Kill Chain

- Reconnaissance: Map network, identify vulnerabilities, identify potential targets, etc.
- Choose weapon: Determine the agent(s) that will perform exploit
- Deliver the weapon to the target
- Exploit the system to execute the weapon
- Install the weapon on target asset(s)
- Command & control of the weapon in the target network – could include laterally propagating the network, installing additional agents, etc.
- Take action using weapon against target asset(s)



Addressing the Cyber Problem

High-Level Steps

- Manage Cyber Risks
  - Accept
  - Avoid
  - Mitigate
  - Transfer
- Requires Senior Leadership Involvement
  - Formally Publish Cyber Policy
  - Regular Cyber Risk Reports
  - Train Employees and Affiliates
  - Enforcement

Addressing the Cyber Problem

Mitigating Common Attack Vectors

- Employee and Affiliate Misuse
  - Formal, published cyber policy with cyber awareness training
  - Test employee / affiliate behavior via simulated attack
  - Log analysis to track behavior in system access
- Phishing
  - Test employee / affiliate behavior via simulated phishing attacks
  - Log analysis to discover phishing attacks and delete / block emails
- Malware
  - Open sources, such as TotalVirus and OTX, provide external threat intel on malware and malicious behavior patterns
  - Data encryption limits scope of data w/o certificate
  - Application whitelist / blacklist … do not allow unauthorized applications
  - Compartmentalized virtual desktop limits scope of malware downloaded from web / email

Addressing the Cyber Problem

Mitigating Common Attack Vectors

- SQL Injection and Cross-Site Scripting
  - Internal penetration testing to discover and fix vulnerable applications
  - Log analysis to discover data exfiltration and break connection
  - Detonation Chamber (application sandbox)
- Brute Password Cracking
  - Enforce password complexity in applications / systems
  - Internal penetration testing to discover and fix vulnerable applications
- Social Engineering Man-in-the-Middle
  - Test employee / affiliate behavior via simulated attack
- Device Theft
  - Device encryption
  - Virtual, compartmentalized workspace

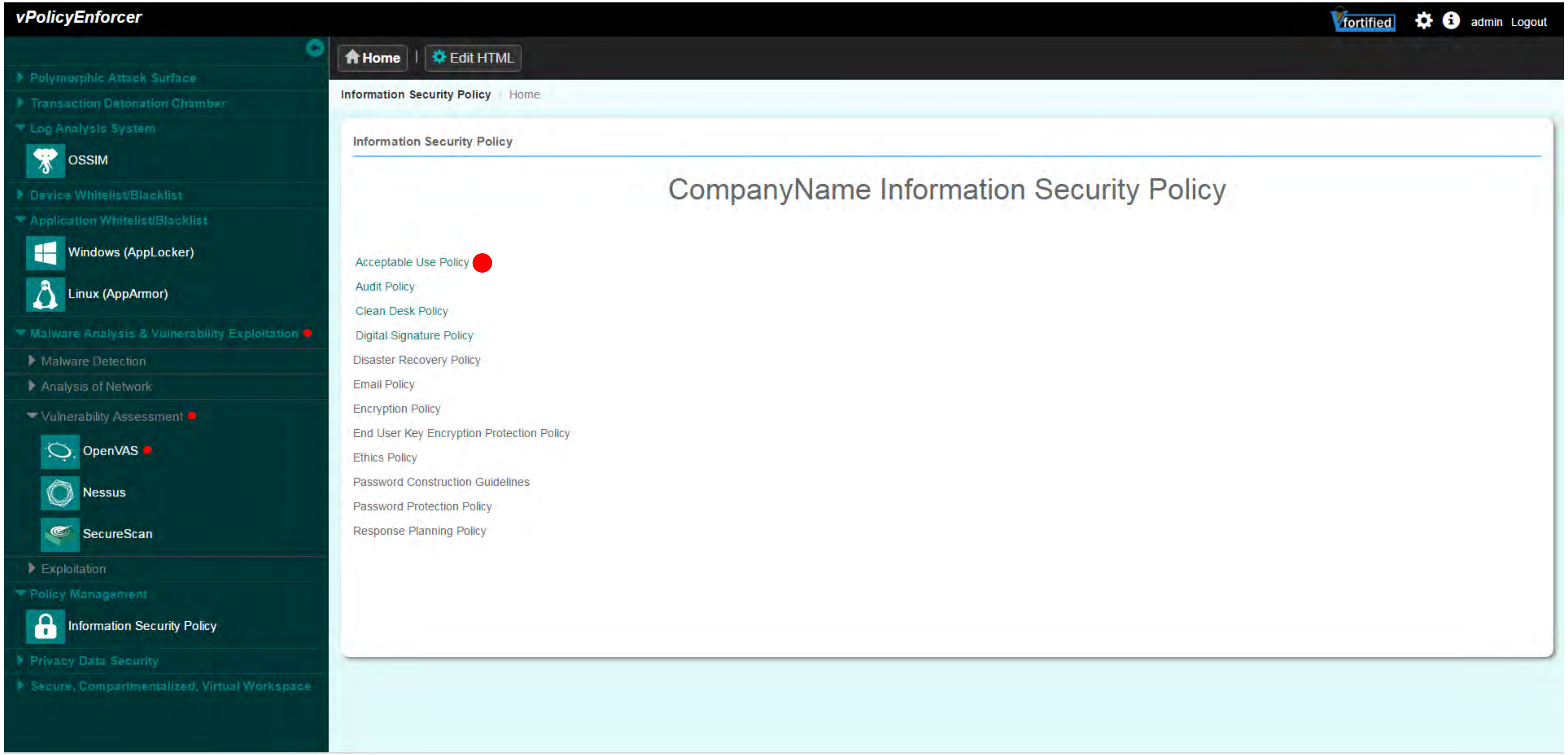
Addressing the Cyber Problem

vPolicyEnforcer Overview

- Complete Tool for SMB
  - **Policy Management (PoM)**: Enforce Cyber from Leader Policy
  - **Malware Analysis and Vulnerability Exploitation (MAVE)**: Low-Hanging Fruit
  - **Log Analysis System (LAS)**: Discover issues through activity patterns
  - **Privacy Data Security (PriDaS)**: Protect Data through Encryption
  - **Device Whitelist / Blacklist (DWB)**: Restrict User Device Access
  - **Application Whitelist / Blacklist (AWB)**: Restrict Applications Access
  - **Polymorphic Attack Surface (PAS)**: Reset the cyber kill chain
  - **Transaction Detonation Chamber (TDC)**: Verify clean transactions using sandbox concept
  - **Secure, Compartmentalized, Virtual Workspace (SCW)**: “Dumb User” Protection
- Easy to Use

Define and Enforce Cyber Policy

Percolate Cyber Status to Management


vPolicyEnforcer
fortified
admin Logout
Home
Edit HTML
Polymorphic Attack Surface
Transaction Detonation Chamber
Log Analysis System
OSSIM
Device Whitelist/Blacklist
Application Whitelist/Blacklist
Windows (AppLocker)
Linux (AppArmor)
Malware Analysis & Vulnerability Exploitation ●
Malware Detection
Analysis of Network
Vulnerability Assessment ●
OpenVAS ●
Nessus
SecureScan
Exploitation
Policy Management
Information Security Policy
Privacy Data Security
Secure, Compartmentalized, Virtual Workspace
Information Security Policy / Home

Information Security Policy

CompanyName Information Security Policy

Acceptable Use Policy ●

Audit Policy

Clean Desk Policy

Digital Signature Policy

Disaster Recovery Policy

Email Policy

Encryption Policy

End User Key Encryption Protection Policy

Ethics Policy

Password Construction Guidelines

Password Protection Policy

Response Planning Policy

Summary

- Cyber is a growing concern for SMBs
  - Attackers have shifted focus to SMBs
    - Access to large business
    - Easier targets
  - Can have devastating effects
- Cyber issues can be resolved
  - Senior leadership policy with enforcement
- vPolicyEnforcer was developed specifically to address unique SMB issues