Agenda

• Steps that can be taken to manage shadow IT
• Common strategies to building a shadow IR Risk Management Program
• How to gain visibility into rogue apps
• The importance of managing shadow IT
• Lessons learned from being in the trenches
• Questions
Introduction

Foundations of Shadow IT defined (in simplest terms)– those employee/vendor owned IT devices brought into your organization's IT environment without:

• Security review to include impact assessments;
• Integration into the security control program; and,
• Following enterprise IT approval processes.

• Would you allow random downloading of any application or software on to your services and endpoints without any review?
• Do you have solid configuration management processes in place? Perhaps not as good as you think.

Let explore Shadow IT and its impacts, both positive and negative, along with managing this ever present reality within our organizations and our business partners, supplies, vendors and contractors.
Statistics

% point impact on firm’s share price on the Friday following the incident

- Retail, hospitality and travel: -0.4%
- Healthcare: -0.7%
- Technology: -2.1%
- Industrial: -2.3%
- Communications: -2.6%
- Financial: -2.7%
Statistics

Sources of security incidents

<table>
<thead>
<tr>
<th>Source</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current employees</td>
<td>35%</td>
<td>34%</td>
</tr>
<tr>
<td>Former employees</td>
<td>30%</td>
<td>29%</td>
</tr>
<tr>
<td>Current service providers/consultants/contractors</td>
<td>18%</td>
<td>22%</td>
</tr>
<tr>
<td>Former service providers/consultants/contractors</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>Suppliers/partners</td>
<td>13%</td>
<td>16%</td>
</tr>
</tbody>
</table>

The most significant cybersecurity challenges:

1. Security protocols/standards of third-party vendors
2. Rapidly evolving, sophisticated, & complex technologies
3. Cross-border data exchanges
4. Increased use of mobile technologies by customers
5. Heightened information security threats from outside the country

PWC 2016 Global State Information Security Survey
Banking and Finance looked good until…

Cybersecurity
China Suspected in FDIC Breaches
by chetrow • July 13, 2016
The Chinese government likely was responsible for the hacking of computers at the Federal Deposit Insurance Corp. in 2010, 2011 and 2013, an audit from the year continued.

Swift CEO to Say More Banks May Have Been Breached by Hackers
by Alan Reda • May 22, 2016
Vendor Related POS breach

Vendor Related POS Breaches

- WORM: 1
- CAPTURE APP: 2
- ADMINWARE: 2
- SPYWARE/KEYLOG: 3
- DOWNLOADER: 4
- CAPTURE: 4
- BACKDOOR: 155
- C2: 160
- EXPORT DATA: 210
- RAMSCRAPER: 512

Verizon 2016 Data Breach Report
IT Vendors and Managed Services Risks

- As were seen in the several retail and service provider breaches, both systems design and vendors were causal factors in these events.
- Insecure system design and lack of third party controls in place.
- The majority of all the vendor related breaches were through stolen credentials that came from legitimate business partner access.
Cloud Service Provider Risk

- Cloud and Managed Service Providers provide critical service to your organization
- To address the Cyber risks associated with these services, Cloud and Managed service providers must meet your Security Policies and Procedures along with operational service level agreements
- Prescreening employees
- Notification of change of employment status
- Approval of maintenance equipment and tools brought into your IT areas
- Managed Security service providers need a higher level of scrutiny
- Assurance of secure code development
Case in Point – Managed service and cloud service providers offer APIs to administer and access managed services.

- Critical security controls depend on these APIs.
- These APIs often have greater exposure of these services to public facing networks.
- Without strong secure coding - insecure interfaces and APIs expose your organizations to security vulnerabilities.
Example

Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

CAPEC-110: SQL Injection through SOAP Parameter Tampering

Attack Pattern ID: 110
Abstraction: Detailed

Presentation Filter: Basic

Summary
An attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack. On the service provider side, the SOAP message is parsed and parameters are not properly validated before being used to access a database in a way that does not use parameter binding, thus enabling the attacker to control the structure of the executed SQL query. This pattern describes a SQL injection attack with the delivery mechanism being a SOAP message.

Attack Prerequisites
- SOAP messages are used as a communication mechanism in the system
- SOAP parameters are not properly validated at the service provider
- The service provider does not properly utilize parameter binding when building SQL queries

Solutions and Mitigations
Properly validate and sanitize/reject user input at the service provider.
Ensure that prepared statements or other mechanism that enables parameter binding is used when accessing the database in a way that would prevent the attackers' supplied data from controlling the structure of the executed query.
At the database level, ensure that the database user used by the application in a particular context has the minimum needed privileges to the database that are needed to perform the operation. When possible, run queries against pre-generated views rather than the tables directly.

Related Attack Patterns
Nature Type ID Name
Tools to identify rogue services

What do you have good asset management?
Roadmap

Vendor/Supplier/Managed Service Mapping to Business Lines

Use Current BIAs to Prioritize Vendors, Suppliers and Manager Service Providers

Analyze Existing Supplier, Vendor Management Policies, Procedures versus Risk Environment

Develop and Implement an Action Plan based on Organization risk

Maintenance - annual assessments
Supplier/Vendor and Manager Service Provider Risk management processes
Roadmap

- Lean and agile supplier/vendor risk management processes that are business enablers
- Manage operations within the risk appetite of management/stakeholders
- Phased approach of implementation building on success – get quick wins to start the process off and solidify stakeholder acceptance
- Update Contracts (Business Associate Agreements, partnering, supplier and vendor contracts) - enable visibility into current and emerging risks
- Vendors and Your Organization performing continuous and regularly scheduled security testing
IT Supplier and Vendor risk management is an enterprise wide effort

Requires clear definition of responsibilities for security for all parties involved

Trust is a natural course of business, but if not verified on a regular on-going basis will lead to possible degradation of your organization’s security posture

Takeaways
Questions
THANK YOU

Justin Orcutt
Justin.Orcutt@nccgroup.trust
470.249.7810

Jeff Roth, CISSP-ISSEP, CISA, CGEIT, QSA
jeff.roth@nccgroup.trust
321.795.0391