The Critical Components of Cyber Security

Ron Hardin, CHTP
Director of Information Technology
Sandestin Investments, LLC

• Cyber Security Plan
• Risk Assessment
• Vulnerability Management
• Training & Awareness Program
• Response & Recovery
HFTP 2019 ANNUAL CONVENTION

ACTION

PLAN

HFTP 2019 ANNUAL CONVENTION

BOTH!

If they’re done right
Cyber Security Plan

Assess

Report

Remediate
What are my information ASSETS?

Which info assets are SENSITIVE?

How do I REDUCE RISK?

Which info assets are VALUABLE?

What are my RISKS?

Where are my info assets stored?

MANAGING RISK

Vulnerability Management Life Cycle

Create Baselines

Monitor

Scan & Ticket

Control

Risk Assessment

Temporary Controls for Critical Risks

Source: Centurion Payments
Assessing the Threat Landscape

2019 Data Breach Investigations Report

Executive Summary

verizon business ready
Summary: Data breaches continue to make headlines around the world. Seemingly, no matter what defensive measures security professionals put in place, attackers are able to circumvent them. No organization is too large or too small to fall victim to a data breach. No industry vertical is immune to attack. Regardless of the type or amount of your organization’s data, there is someone out there who is trying to steal it. Having a sound understanding of the threats you and your peer organizations face, how they have evolved over time, and which tactics are most likely to be utilized can prepare you to manage these risks more effectively and efficiently.
Verizon 2019 DBIR – Key Takeaways

• Take Me To Your Leader
• Get Out of My Cloud
• What a Tangled Web We Weave
• Still Held For Ransom
• Chip and Pin For the Win?
• HR Strikes Back
• I Click, Therefore I Am

Risk Assessment (cont’d)

Talk to Your Lawyer
# Risk Assessment

## Legal & Regulatory Requirements

### Contractual Obligations

![PCI logo]

---

## State Comprehensive-Privacy Law Comparison

*Source: [https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf](https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf)*

<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Process</th>
<th>Statute/Bill</th>
<th>Common Name</th>
<th>Consumer Rights</th>
<th>Business Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td></td>
<td>Ca. Civ. Code §§ 1798.100 - 199</td>
<td>California Consumer Privacy Act</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Connecticut</td>
<td></td>
<td>HB 1108</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hawaii</td>
<td></td>
<td>SB 418</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illinois</td>
<td></td>
<td>HB 3358</td>
<td>Data Transparency and Privacy Act</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Louisiana</td>
<td></td>
<td>HB 465¹</td>
<td>Internet and Social Media Privacy and Protection Act</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maine</td>
<td></td>
<td>LD 946²</td>
<td>An Act To Protect the Privacy of Online Consumer Information</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

1. [link to legislation](https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf)
2. [link to legislation](https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf)
<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Process</th>
<th>Statute/Bill</th>
<th>Common Name</th>
<th>Consumer Rights</th>
<th>Business Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maryland</td>
<td>SB 613</td>
<td>Online Consumer Protection Act</td>
<td></td>
<td>x x x x x</td>
<td></td>
</tr>
<tr>
<td>Massachusetts</td>
<td>SD 4312/JS 120</td>
<td></td>
<td></td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Minnesota</td>
<td>HF 2872/SP 2012</td>
<td></td>
<td></td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Nevada</td>
<td>SB2200/Chapter 405A</td>
<td></td>
<td></td>
<td>x x x</td>
<td></td>
</tr>
<tr>
<td>New Jersey</td>
<td>SB 884A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nevada</td>
<td>SB 4H3</td>
<td>Consumer Information Privacy Act</td>
<td></td>
<td>x x x</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>SB 5562**</td>
<td>New York Privacy Act</td>
<td></td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>North Dakota</td>
<td>HB 6560**</td>
<td></td>
<td></td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>HB 1549</td>
<td>Consumer Data Privacy Act</td>
<td></td>
<td>x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>SB 1344</td>
<td>Consumer Privacy Protection Act</td>
<td></td>
<td>x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Texas</td>
<td>HB 4518</td>
<td>Texas Consumer Privacy Act</td>
<td></td>
<td>x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Texas</td>
<td>HB 1360**</td>
<td>Texas Privacy Protection Act</td>
<td></td>
<td>x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Washington</td>
<td>SB 5396</td>
<td>Washington Privacy Act</td>
<td></td>
<td>x x x x</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>

1 Louisiana HB 465 applies only to internet service providers, internet service operators, and social media companies.
2 Maine LD 946 applies only to internet service providers.
3 New York SB 55642 includes a broad consumer right to opt-out of any processing, not just the sale of personal information.
4 North Dakota HB 1485 is a broad prohibition on disclosure of personal information except upon explicit consent.
5 Texas HB 4380 is a GDPR-style restriction-based bill that prohibits a business from collecting or processing information except under certain circumstances.

Legislative Process: Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

Last updated: 7/31/2019
Vulnerability Management

- Threat intelligence & alerting
- Vulnerability scanning
- Patch management
- Penetration testing
- Anti-malware
- Configuration & change management
Threat Intelligence & Alerting

AA19-168A: Microsoft Operating Systems BlueKeep Vulnerability
AA19-122A: New Exploits for Unsecure SAP Systems
AA19-024A: DNS Infrastructure Hijacking Campaign
AA18-331A: SamSam Ransomware
TA18-331A: 3ve – Major Online Ad Fraud Operation
AA18-284A: Publicly Available Tools Seen in Cyber Incidents Worldwide
TA18-276B: Advanced Persistent Threat Activity Exploiting Managed Service Providers
TA18-276A: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation
TA18-275A: HIDDEN COBRA – FASTCash Campaign
TA18-201A: Emotet Malware
TA18-149A: HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm
TA18-145A: Cyber Actors Target Home and Office Routers and Networked Devices Worldwide
TA18-141A: Side-Channel Vulnerability Variants 3a and 4
TA18-106A: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
TA18-086A: Brute Force Attacks Conducted by Cyber Actors
TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors
TA18-004A: Meltdown and Spectre Side-Channel Vulnerability Guidance
TA17-315B: HIDDEN COBRA – North Korean Trojan: Volgmer
TA17-315A: HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL
TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors
TA17-181A: Petya Ransomware
Alert (AA19-168A)

Microsoft Operating Systems BlueKeep Vulnerability

Original release date: June 17, 2019

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this Activity Alert to provide information on a vulnerability, known as “BlueKeep,” that exists in the following Microsoft Windows Operating Systems (OSs), including both 32- and 64-bit versions, as well as all Service Pack versions:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

An attacker can exploit this vulnerability to take control of an affected system.

Technical Details

BlueKeep (CVE-2019-0708) exists within the Remote Desktop Protocol (RDP) used by the Microsoft Windows OSs listed above. An attacker can exploit this vulnerability to perform remote code execution on an unprotected system.

According to Microsoft, an attacker can send specially crafted packets to one of these operating systems that has RDP enabled. After successfully sending the packets, the attacker would have the ability to perform a number of actions: adding accounts with full user rights; viewing, changing, or deleting data; or installing programs. This exploit, which requires no user interaction, must occur before authentication to be successful.

BlueKeep is considered “wormable” because malware exploiting this vulnerability on a system could propagate to other vulnerable systems; thus, a BlueKeep exploit would be capable of rapidly spreading in a fashion similar to the WannaCry malware attacks of 2017.
Mitigations
CISA encourages users and administrators to review the Microsoft Security Advisory and the Microsoft Customer Guidance for CVE-2019-0708 and apply the appropriate mitigation measures as soon as possible:

- **Install available patches.** Microsoft has released security updates to patch this vulnerability. Microsoft has also released patches for a number of OSs that are no longer officially supported, including Windows Vista, Windows XP, and Windows Server 2003. As always, CISA encourages users and administrators to test patches before installation.

For OSs that do not have patches or systems that cannot be patched, other mitigation steps can be used to help protect against BlueKeep:

- **Upgrade end-of-life (EOL) OSs.** Consider upgrading any EOL OSs no longer supported by Microsoft to a newer, supported OS, such as Windows 10.
- **Disable unnecessary services.** Disable services not being used by the OS. This best practice limits exposure to vulnerabilities.
- **Enable Network Level Authentication.** Enable Network Level Authentication in Windows 7, Windows Server 2008, and Windows Server 2008 R2. Doing so forces a session request to be authenticated and effectively mitigates against BlueKeep, as exploit of the vulnerability requires an unauthenticated session.
- **Block Transmission Control Protocol (TCP) port 3389 at the enterprise perimeter firewall.** Because port 3389 is used to initiate an RDP session, blocking it prevents an attacker from exploiting BlueKeep from outside the user’s network. However, this will block legitimate RDP sessions and may not prevent unauthenticated sessions from being initiated inside a network.
Vulnerability Scanning

- External Scanning
- Discovery/Validation
- PCI ASV Quarterly Scanning
- General External Scanning
- Internal Scanning
- Endpoint Management
2 Penetration Testing Components

The goals of penetration testing are:

1. To determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data.

2. To confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation, required in PCI DSS are in place.
Black-box: the entity provides no information prior to the start of testing.
White-box: the entity may provide the penetration tester with full and complete details of the network and applications.
Grey-box: the entity may provide partial details of the target systems.

PCI DSS penetration tests are typically performed as either white-box or grey-box assessments. These types of assessments yield more accurate results and provide a more comprehensive test of the security posture of the environment than a pure black-box assessment. Black-box assessments offer very little in the way of value for PCI DSS penetration tests, since the entity provides no details of the target systems prior to the start of the test, the test may require more time, money, and resources to perform.
Patch Management

- Frequently combined with scanning in a Vulnerability Management platform
- Manual or automated?
- ANY patching and updating is BETTER than NO PATCHING
- PCI 30-day critical patch requirement
A vulnerability management program typically consists of the following steps:

- Identify vulnerabilities through vulnerability scanning and penetration testing.
- Identify patches for vulnerabilities from vendor announcements.
- If a patch is not available, develop mitigation plan to mitigate the risk of not having a patch.
- Review vulnerabilities and adjust CVSS scores based on applicability to organization’s environment.
- Test patches.
- If a patch fails testing, develop mitigation plan to mitigate the risk of not being able to apply the patch.
- Patch systems with compatible patches and implement mitigation plans for patches that cannot be applied.

How to mitigate vulnerabilities?

- Create or tweak your log analysis rules to look for any indications that the risk is being exploited.
- Use a white or blacklisting application to monitor for any changes to the device.
- Use host intrusion detection system (HIDS) to monitor for exploits.
- Further lock down firewall rules to restrict access to suspect IP addresses used by exploits.
- Make sure that your detection processes function in near real time so that you are getting notification as soon as possible. Waiting for a daily or even weekly review of information generated by these mitigation techniques is just too late since the compromise will likely be long over by that time.
• LOTS of options, ranging from free to very expensive
• Business versions of consumer-oriented products
• Multi-function endpoint-protection suites – hosted or on-premise
• Windows Defender is getting better, but all top 3\textsuperscript{rd}-party products outperform it (according to PC Magazine 2019 review)
• Lots of variability in features
• Parallel point products such as anti-ransomware available at low cost
Anti-Malware

- PCI DSS requires anti-malware software on all at-risk devices
- Also requires that A-M be managed and monitored to ensure it is active, working, and updated
- An endpoint management or network access control system can enforce the A-M requirement

Most ransomware and destructive malware attacks would be prevented by active anti-malware and fully-patched computers.
Configuration & Change Management

JUST DO IT

Training & Awareness
• Most attacks use malware
• Most malware gets in via phishing
  (or other social-engineering techniques)
• The most effective defense against phishing
  and social engineering is an ongoing program
  of SECURITY TRAINING AND AWARENESS

Any Questions?
Training & Awareness

• Phishing campaigns and other social engineering exercises
• Basic and remedial training
• Online, quick and engaging
• Significant improvement in just one round

Response and Recovery
• How good are your backups?
• Are your backups protected?
• Do you have a DR plan integrated with backups?
• Do you have an incident response plan?
• Do you have comprehensive downtime plans?
Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminate ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.

How is Ransomware Spread?

• Email phishing campaigns, increasingly targeted at specific organizations
• Exploitation of Remote Desktop Protocol
• Exploitation of software vulnerabilities
IF MY SYSTEM IS INFECTED, SHOULD I PAY THE RANSOM?
The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

HOW CAN I PROTECT MYSELF AGAINST RANSOMWARE?
The most important defense for any organization against ransomware is a robust system of backups. Having a recent backup to restore from could prevent a ransomware attack from crippling your organization. The time to invest in backups and other cyber defenses is before an attacker strikes, not afterward when it may be too late.
CYBER DEFENSE BEST PRACTICES

- Regularly backup data and ensure its integrity
- Ensure backups are protected
- Focus on awareness and training
- Patch the OS, software, and firmware on all devices
- Use a centralized patch management system

- Ensure anti-malware solutions are set to automatically update and scan regularly
- Implement the *least privilege* for file, network, and share permissions
- Disable macro scripts for Office files transmitted by email
CYBER DEFENSE BEST PRACTICES

• Consider using Office Viewer software for Office files received via email
• Implement software restriction policies that prevent execution in common malware locations
• Employ best practices for use of RDP

• Use 2-factor authentication for RDP and other remote access tools
• Implement application whitelisting
• Leverage virtualization to protect environment from unauthorized changes like encryption
• Categorize data and use network segmentation to secure valuable/sensitive data
CYBER DEFENSE BEST PRACTICES

• Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall. For example, require users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.

Any Questions?