Cybercrime Series
The 2017 Cybersecurity Landscape

4/27/2017 - NJAMHAA IT Annual Conference
The 2017 Cybersecurity Landscape and HIPAA Compliance
Cybercrime Overview

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker.
- Your unprotected PC can become infected within four minutes of connecting to the Internet.
- Average total cost of a data breach increased from $3.52 million in 2014 to $3.79 million in 2015.
- Cybercrime will become a $2.1 trillion industry by 2019.
- The Dark Web: [https://torflow.uncharted.software/#/2015-12-8](https://torflow.uncharted.software/#/2015-12-8)
Even if they don’t want your data...they know YOU want your data
The 800lb Gorilla, Ransomware!

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet. The server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay $300 USD / 300 EUR / similar amount in another currency.

Click «next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
The 800lb Gorilla, Ransomware!

4/14/2015
03:16 PM

Police Pay Off Ransomware Operators, Again

Law enforcement agencies are proving to be easy marks -- but are they any worse than the rest of us?

Police departments are proving to be easy marks for ransomware operators -- but perhaps no more so than anyone else. Recently, reports are stacking up of police departments paying attackers ransoms -- payments in the $300 to $500, made in Bitcoins -- for the recovery of encrypted files and equipment.

Despite having certain resources readily available -- like assistance from FBI investigators, for example -- police aren't faring any better than the private sector against ransomware.

But are they faring any worse? Are police departments more likely to be infected, less likely to have good backups and restores, or generally more willing to pay criminals? Or are we just more likely to hear about these incidents because they are public entities, while such events go unreported when they occur in the private sector?
'Ransomware' software attacks stymie law firms

In the annals of Internet crime, "ransomware"—software that freezes up a computer, encrypts all its data and demands a ransom for the system's restoration—is especially malicious. And attorneys are among the targets.

David J. Bilinsky, adviser and staff lawyer at the Law Society of British Columbia, says one of its member firms suffered a hostile takeover of its computers by ransomware late last year. Bilinsky says the attack came on the heels of ransomware takedowns at two other member law firms in 2013.

"These attacks emphasize the need for law firms of all sizes to increase their awareness and implementation of current security protocols," Bilinsky says.

And this problem doesn't stop above the U.S. border. "I know one technology and forensics consultant in Virginia who has helped at least 50 firms across many states," says Dan Finnington, vice president of claims prevention and stakeholder relations at the Lawyers' Professional Indemnity Co. "I know many of my practice management adviser colleagues at the various state bar associations have taken calls from firms that have been infected."
The 800lb Gorilla: Ransomware!

Hotel ransomed by hackers as guests locked out of rooms

One of Europe's top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)
ON TARGET

The 800lb Gorilla, Ransomware!

Spencer Chamber of Commerce Infected With Ransomware

November 18, 2016  Kayla Thrallkill
The 800lb Gorilla, Ransomware!

‘You Hacked’ appears at Muni stations as fare payment system crashes

By Joe Fitzgerald Rodriguez on November 26, 2016 3:10 pm

That was part of the message displayed on computer screens at Muni stations across San Francisco on Saturday in what appears to be a computer hack targeting The City.

Along with the message, fare payment machines at Muni underground stations read, “OUT OF SERVICE” in red LED letters.
The 800lb Gorilla, Ransomware!

HACKED HOSPITAL RANSOM PAYOUT WILL CAUSE ‘PROLIFERATION OF ATTACKS’

BY ANTHONY CUTHBERTSON ON 2/16/16 AT 1:06 PM

The Hollywood Presbyterian Medical Center is pictured in Los Angeles, California February 16. A cyber attack that crippled the hospital's electronic database led to a $17,000 ransom pay out to hackers.
The 800lb Gorilla, Ransomware!

SamSam: The Doctor Will See You, After He Pays The Ransom

Cisco Talos is currently observing a widespread campaign leveraging the Samas/Samsam/MSIL.B/C ransomware variant. Unlike most ransomware, SamSam is not launched via user focused attack vectors, such as phishing campaigns and exploit kits. This particular family seems to be distributed via compromising servers and using them as a foothold to move laterally through the network to compromise additional machines which are then held for ransom. A particular focus appears to have been placed on the healthcare industry.

Adversaries have been seen leveraging JexBos, an open source tool for testing and exploiting JBoss application servers, to gain a foothold in the network. Once they have access to the network they proceed to encrypt multiple Windows systems using SamSam.
The 800lb Gorilla, Ransomware!

Estimated over $1 Billion paid in ransom in 2016!
The 800lb Gorilla, Ransomware!

Ransomware Spiked 752% in New Families in 2016

In a span of 12 months, the number of discovered ransomware families jumped from 29 to 247. This marks a 752% increase compared to the volume of ransomware families detected in 2015.

Estimated over $1 Billion paid in ransom in 2016!
The 800lb Gorilla, Ransomware!

Ransomware targets a wide variety of industries

Of the customers who have experienced ransomware attacks, what industries were they within?

- Consumer Products: 23%
- Tech / Computer Services: 21%
- Industrial, Construction, & Manufacturing: 20%
- Professional Services: 20%
- Finance & Insurance: 19%
- Healthcare: 15%
- Media & Entertainment: 14%
- Architecture & Design Services: 10%
- Energy & Utilities: 10%
- Government: 10%
- Non-Profit: 10%
- Retail: 10%
- Real Estate: 9%
- Legal: 6%
- Telecom: 6%
- Travel & Transportation: 6%
- Education: 4%
- Other: 1%

datto
And NO, a good Backup isn’t good enough
The 800lb Gorilla, Ransomware!

Which of the following, if any, have you experienced while assisting a customer with ransomware?

- Data and/or Device was Lost: 58%
- Business-Threatening Downtime: 45%
- Paid a ransom and recovered the data: 17%
- Paid a ransom but data was never released: 14%

datto
The 800lb Gorilla, Ransomware!

100% Reputational Risk

Which of the following, if any, have you experienced while assisting a customer with Ransomware?

- Data and/or Device was Lost: 58%
- Business-Threatening Downtime: 45%
- Paid a ransom and recovered the data: 17%
- Paid a ransom but data was never released: 14%

datto
Meet Jigsaw

- Threatens to release your data to the public on the "dark web"
- Countdown clock where it permanently deletes files over time to instill urgency
6. Is it a HIPAA breach if ransomware infects a covered entity’s or business associate’s computer system?

Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” See 45 C.F.R. 164.402.⁶

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized

⁶ See also Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act.
Meet Breach notices

7. How can covered entities or business associates demonstrate “...that there is a low probability that the PHI has been compromised” such that breach notification would not be required?

To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.
Meet Breach notices

According to the NJ Identity Theft Prevention Act:

Any business or public entity required under this section to disclose a breach of security of a customer’s personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

To meet this statutory requirement, please report security breaches to databreach@cyber.nj.gov.

NJ 56:8-163 Disclosure of breach of security to customers.

12. a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
People are (still) the biggest security risks

Social engineering and 'download this attachment' scams are back – as if they ever left – and working better than ever, unfortunately.
<table>
<thead>
<tr>
<th>Application</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email link</td>
<td>31%</td>
</tr>
<tr>
<td>Email attachment</td>
<td>28%</td>
</tr>
<tr>
<td>A Web site or Web application other than email or social media</td>
<td>24%</td>
</tr>
<tr>
<td>Social media</td>
<td>4%</td>
</tr>
<tr>
<td>USB stick</td>
<td>3%</td>
</tr>
<tr>
<td>Business application</td>
<td>1%</td>
</tr>
<tr>
<td>We don’t know</td>
<td>9%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*
The Threat Landscape: Phishing

Online Banking Alert

Unlocking Your Online Banking

Dear Bank of America Customer,

There are a number of ways to keep your account secure. We'd like to remind you that we need to verify your identity before we can assist you. If you have not yet done so, please verify your identity via e-mail. If you have already done so, please follow the instructions below.

Please click here to continue the verification process and ensure your account security.

Thank you for your cooperation.

Want to get more alerts? Sign in to Bank of America Online Banking and select the "Security Alerts" icon in the "Security Center." 

Terms & Conditions | Site Map | Privacy Policy | Phishing Policy 2014 E-ZPass
The Threat Landscape: Malvertising

**What is Malvertising?**

Malicious advertising ("malvertising") is a type of online attack wherein malicious code hidden within an online ad infects your computer with malware.

**How Malvertising Works**

You visit a website. It doesn’t matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.

**Malicious Bidding**

Cyber criminals are able to utilize malvertising by submitting good-faith dropped advertisements to ad networks for a real-time bidding process.

After the ad wins the bid, it is propagated in real time through various publishers and will only trigger its malicious payload if specific conditions are met.

**Hard to Catch**

Malicious ads rotate in with normal ads. Therefore, when a user visits an infected site, they might not be alerted.

Because duplicating the infection is difficult, this can make it very hard for security researchers to study a malvertising attack.

**Protection**

Using software like pop-up/ad blockers offers some protection against malvertising, but employing anti-exploit software in conjunction with an anti-malware is your best bet.

Learn more at www.malwaredbytes.org.
The Threat Landscape: Social Media
Stay Patched!

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>2015 vs. 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>47%</td>
<td>▼</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>73%</td>
<td>▼</td>
</tr>
<tr>
<td>Office®</td>
<td>53%</td>
<td>▼</td>
</tr>
<tr>
<td>Windows</td>
<td>26%</td>
<td>▼</td>
</tr>
<tr>
<td>Edge</td>
<td>2,100%</td>
<td>▲</td>
</tr>
<tr>
<td>MSXML</td>
<td>100%</td>
<td>▼</td>
</tr>
<tr>
<td>Chakra</td>
<td>100%</td>
<td>▲</td>
</tr>
<tr>
<td>.NET</td>
<td>100%</td>
<td>▲</td>
</tr>
<tr>
<td>Reader</td>
<td>100%</td>
<td>▲</td>
</tr>
<tr>
<td>Windows Media® Center</td>
<td>100%</td>
<td>▲</td>
</tr>
<tr>
<td>ODays</td>
<td>17%</td>
<td>▼</td>
</tr>
<tr>
<td>Android</td>
<td>206%</td>
<td>▲</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>2015 vs. 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>8%</td>
<td>▼</td>
</tr>
<tr>
<td>Flash</td>
<td>43%</td>
<td>▼</td>
</tr>
<tr>
<td>Acrobat Reader DC</td>
<td>0%</td>
<td>—</td>
</tr>
<tr>
<td>Acrobat Pro DC</td>
<td>133%</td>
<td>▲</td>
</tr>
<tr>
<td>Digital Edition</td>
<td>200%</td>
<td>▲</td>
</tr>
<tr>
<td>Creative Cloud®</td>
<td>100%</td>
<td>▲</td>
</tr>
<tr>
<td>Apple</td>
<td>145%</td>
<td>▲</td>
</tr>
<tr>
<td>iOS®</td>
<td>275%</td>
<td>▲</td>
</tr>
<tr>
<td>OS X</td>
<td>189%</td>
<td>▲</td>
</tr>
<tr>
<td>QuickTime®</td>
<td>57%</td>
<td>▼</td>
</tr>
<tr>
<td>Safari®</td>
<td>175%</td>
<td>▲</td>
</tr>
<tr>
<td>SCADA</td>
<td>421%</td>
<td>▲</td>
</tr>
</tbody>
</table>

Table 2. Trend Micro and ZDI (with TippingPoint) discovered vulnerabilities 2015 versus 2016
The Threat Landscape: Internet

What do the 6 most popular sites on the internet have in common?

- **https - they are encrypted**
- Your firewall cannot scan encrypted traffic from the internet
- Popular way cybercriminals get in - Hide code in encrypted sites
- Ransomware’s top entry method
Who has the following?
THE INTERNET OF THINGS
<table>
<thead>
<tr>
<th>Username/Password</th>
<th>Manufacturer</th>
<th>Link to supporting evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/123456</td>
<td>ACTI IP Camera</td>
<td><a href="https://sipcam.com/docs/ip-cameras-default-passwords-directory">https://sipcam.com/docs/ip-cameras-default-passwords-directory</a></td>
</tr>
<tr>
<td>root/askus</td>
<td>Alex IP Camera, et. al</td>
<td><a href="http://www.dlink.com/router-default.UTF8/0563-001">http://www.dlink.com/router-default.UTF8/0563-001</a></td>
</tr>
<tr>
<td>root7/M0o0vizv</td>
<td>Dahua Camera</td>
<td><a href="http://www.dahua.com/index.php?option=93666">http://www.dahua.com/index.php?option=93666</a></td>
</tr>
<tr>
<td>root7/M0o0vahuid</td>
<td>Dahua IP Camera</td>
<td><a href="http://www.dahua.com/index.php?option=93966">http://www.dahua.com/index.php?option=93966</a></td>
</tr>
<tr>
<td>root/dr3embox</td>
<td>Dreambox TV receiver</td>
<td><a href="https://www.satellites.co.uk/forums/threads/reset-cool-password-plugin.101140">https://www.satellites.co.uk/forums/threads/reset-cool-password-plugin.101140</a></td>
</tr>
<tr>
<td>root/ezx</td>
<td>EZ XL Two-way Speaker</td>
<td>?</td>
</tr>
<tr>
<td>root/juangchong</td>
<td>Guangzhou Jian Optical</td>
<td><a href="https://news.ycombinator.com/item?id=11114012">https://news.ycombinator.com/item?id=11114012</a></td>
</tr>
<tr>
<td>root/kwe 6318</td>
<td>HiSilicon IP Camera</td>
<td><a href="https://access.iknow.com/201408/27/05-go-on-the-h3318-lp-camera-module/">https://access.iknow.com/201408/27/05-go-on-the-h3318-lp-camera-module/</a></td>
</tr>
<tr>
<td>root/lv123</td>
<td>HiSilicon IP Camera</td>
<td><a href="https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d">https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d</a></td>
</tr>
<tr>
<td>root/lv1234</td>
<td>HiSilicon IP Camera</td>
<td><a href="https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d">https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d</a></td>
</tr>
<tr>
<td>root/lv123rd</td>
<td>HiSilicon IP Camera</td>
<td><a href="https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d">https://git.gitee.com/yabob/1464658537/100f75668e/47f84720f75619b8c7612f7d</a></td>
</tr>
<tr>
<td>root/adminsm</td>
<td>Mobotix Network Camera</td>
<td><a href="http://www.fourm-use-ip.co.uk/threads/mobotix-default-passwords.786">http://www.fourm-use-ip.co.uk/threads/mobotix-default-passwords.786</a></td>
</tr>
<tr>
<td>root/realtek</td>
<td>RealTek Trexiet</td>
<td></td>
</tr>
<tr>
<td>root/adminncunm</td>
<td>SMC Routers</td>
<td><a href="http://www.cleancam.com/views/default/5SMCR">http://www.cleancam.com/views/default/5SMCR</a> ROUTER</td>
</tr>
<tr>
<td>root/supervisor</td>
<td>VideoIQ</td>
<td><a href="https://ipcam.com/reviews/ip-cameras-default-passwords-directory">https://ipcam.com/reviews/ip-cameras-default-passwords-directory</a></td>
</tr>
</tbody>
</table>
Blue Iris Login
70.35.110.45
shdylgtb.com

HTTP/1.1 200 OK
Server: BlueIris-HTTP/1.1
Date: Wed, 19 Apr 2017 18:58:45 GMT
P3P: CP="CAO COR CURa ADMa DEVa OUR IND ONL COM DEM PRE"
Access-Control-Allow-Origin: *
Set-Cookie: session=72c2559b8e60b611e5a3b4823e57a6b; path=/
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

24.144.103.171
user-2089t09p.com
EarlLink

HTTP/1.1 501 Not Implemented
Server: BlueIris-HTTP/1.1
Date: Wed, 19 Apr 2017 18:49:28 GMT
P3P: CP="CAO CURa ADMa DEVa OUR IND ONL COM DEM PRE"
Access-Control-Allow-Origin: *
Set-Cookie: session=72c2559b8e60b611e5a3b4823e57a6b; path=/
Connection: Close

190.218.148.11
cpe-0206a3127210.cpe.cableanda.net

HTTP/1.1 401 Unauthorized
Server: BlueIris-HTTP/1.1
Date: Wed, 19 Apr 2017 18:49:25 GMT
P3P: CP="CAO CURa ADMa DEVa OUR IND ONL COM DEM PRE"
Access-Control-Allow-Origin: *
Set-Cookie: path=/
Connection: Close
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, no-store
W...
AidaBraids is Jacksonville's Authentic African Hair Braiding Shop. – Aida's Authentic Braiding, Florida &8211; African Hair Braiding Shop

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 19 Apr 2017 19:20:25 GMT
Content-type: text/html; charset=UTF-8
Transfer-encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding

301 Moved Permanently
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 19 Apr 2017 19:20:17 GMT
Content-type: text/html
Content-Length: 178
Connection: keep-alive
Location: https://104.131.73.240/
Business Email Compromise

Fri 1/29/2016 12:26 AM

Fund Transfer

To: Rashaad Bajika

You replied to this message on 1/30/2016 2:24 PM.

Rashaad

Can you transfer US$ 1780.00 to the following account from the \[redacted\] account. I tried doing it, wasn’t able to for some reason.

Beneficiary/Account name: \[redacted\]
Beneficiary Address: \[redacted]\nAccount Number: 100\[redacted]\nTransit Number: 0025\[redacted]\nInstitution Number: 003
Bank Name: RBC Royal Bank
Bank Branch Address: \[redacted]\nSwift Code: RO\[redacted]

Thanks a bunch, once done let me know

Regards
June 14, 2016

Alert Number:
I-061416-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.
Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim’s normal business practices.

STATISTICAL DATA

The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses². The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong.
Business Email Compromise

An estimated 25% of US companies have already been targeted

Average loss according to the FBI is $25k - $75k.

Largest “CEO Fraud” Email reported losses to date:

- Scoular $17.2 million (US)
- Ubiquiti $46.7 million (US)
- FACC $54 million (Austria)
- Crelan Bank $76 million (Belgium)
What can your firm do?
Mitigating Risk

- CyberRisk Insurance
- Technology Best Practices
- User Education
Fixes don’t have to be expensive

From Verizon Breach Investigations Report:

But surely after examining another 800 breaches in the past year, we'd have plenty of new recommendations to solve all your security woes, right? Quite wrong, actually. The latest round of evidence leads us to the same conclusion as before: your security woes are not caused by the lack of something new (Figure 43 looks about like it always does). They almost surely have more to do with not using, under using, or misusing something old.
Fixes don’t have to be expensive
Fixes don’t have to be expensive

The biggest security risk is in lack of manpower and knowledge, not technologies.
Layered Security - Defense in Depth - FREE Layers

Remove Administrative Rights - nobody should have them for daily computer use (including System Administrators!)

Lock down Service Accounts - account logon restrictions, no RDP access, unique passwords/logons for each Admin, change default passwords

Principle of Least Privilege - users should have access to minimum resources they need to perform their job. Least amount of files, least amount of websites, least amount of rights.

Password Policy - apply using group policy - Minimum 8 characters, complexity, max age 90 days, account lockout

Patch Management - WSUS, SCCM or alternative solution to make sure all software is patched and up-to-date. 100% certainty no gaps on external facing systems.
Layered Security - Defense in Depth - FREE Layers

Computer Lockout after Inactivity- via Group Policy on all PCs and servers

Windows Firewall - enabled on all PCs via Group Policy, port/service exceptions only via GP

Services Baseline - stop or remove unnecessary services. Server 2016 is more secure by default however can use Security Configuration Wizard to assist in creating hardened baseline configuration.

Security Awareness Training - the biggest vulnerability in most systems are the users. You must have regular training to expose them to best practices and how to identify risks.

Encrypt Data - at critical data at rest and in transit. Email, PII, PHI, etc.
Layered Security - Defense in Depth - FREE Layers

**White Hat Social Engineering** - test the effectiveness of your user’s security awareness. Send “white hat” phishing emails to see which users need more limitations or training.

**Software Restriction Policies** - limit what software can run on computers using Local or Group policy

**AppLocker** - better than Software Restriction Policies. Rather than just stopping “Known Bad” software it can be set to audit usage and then only allow “Known Good” based on Publisher or digital signature. Built into Windows Server 2016 however requires Windows 7/8/10 Enterprise or Ultimate on desktops that will be locked down.
Layered Security - Defense in Depth
Additional Recommended Layers

**Hardware Firewall** - configured with “Deny All” rules and then ports opened up only as needed

**Network Antivirus / AntiMalware** - only catch 10%-40% of threats however still a mandatory first level of defense. Scan compressed files, block those w/passwords.

**AntiSpam/AntiVirus Email Filter** - email is still the most popular threat distribution model. A good email filter can eliminate 98%+ of email phishing and virus threats. Block compressed files w/passwords. Block bad attachment types.

**Internet Content Filter** - must have for all Internet connected PCs.

**Multifactor Authentication** - must have for all remote access

**Vulnerability Scan** - quarterly/annual to confirm no open Windows to the outside

**Basic Monitoring** - Executables, DLLs, processes, patches, network traffic

**Advanced Monitoring** - IPS, IDS, Sandbox, DLP etc

**Windows PowerShell** - the newest attack vector to bypass detection - secure Execution Policy only!

**Good Backup** - at a minimum. Not defense, simply recovery if your defense layers were not sufficient. Still exposed to reputational risk, liability, breach notices, downtime, etc.
HIPAA Guidelines - Ransomware:

- Presence of Ransomware alone is not a breach
- When unprotected (non-encrypted) ePHI is encrypted due to Ransomware a breach has occurred

  - However a breach notification may NOT be required if you can show “there is a low probability that the PHI has been compromised”
    - For example:
      - Mitigation and identification of Ransomware as a variant that does NOT exfiltrate data AND
      - Network monitoring that would detect exfiltration or access of data
      - Network safeguards (block TOR) that would prevent exfiltration
Mitigation Tactics - Ransomware flavors:

**CryptoLocker**  **TeslaCrypt 1.0-4.0**  **AlphaCrypt**  **CryptoWall 1.0-4.0**

**Jigsaw**  **TorrentLocker (CryptoLocker copycat)**

**CryptXXX**  **Cerber**  **Locky**

- Inspect SSL traffic!
- Encrypt your ePHI! - at rest, in transit, in email
- Principle of Least Privilege to limit damage
- Email attachment scanning/blocking - prohibit risky file types and password protected ZIP
- Web Content filter for ALL users
- Patch Windows, Java, etc. - exploit kits are 2nd most common attack vector after email attachments or links
- Unmapping drives is no longer sufficient; newer variants of Locky, Cerber and others can go after UNC paths
- Similar to unmapping network drives, “Canary in the coal mine” files may provide limited benefit
- Monitor for / prohibit:
  - TOR/I2P traffic
  - Encrypted Key Exchange
  - Files running from %AppData% and subfolders
- Some of the older ransomware flavors CAN be decrypted since keys have been recovered
- White Hat Social Engineering - the human firewall!
What is Tor and how does it work?

How Tor Works:

After obtaining a list of Tor nodes from a directory server, the user's Tor client picks a random series of Tor nodes to the destination server.

If the user visits another site at a later time, a second random path will be chosen to the new destination.
Mitigation Tactics - Business Email Compromise

- Human processes are the answer (separation of duties, out of band verification)
- Email authenticity validation (SPF, DKIM, DMARC, etc)
- Multifactor for email
- Whitehat Social engineering
- CyberRisk Insurance
HIPAA Guidelines - Business Email Compromise:

- Check your Cybersecurity policy - it may not cover Business Email Compromise

- If staff is tricked into wiring funds to a rogue 3rd party there is no HIPAA breach or notification requirement

- If staff is tricked into wiring ePHI or PII to a rogue 3rd party there is a HIPAA and/or NJ Consumer Fraud Protection breach and notification requirement
Conclusion

Exploits, Ransomware and Viruses are NOT inevitable
Exploits, Ransomware and Viruses are NOT inevitable.

The biggest security risk is in lack of manpower and knowledge, not technologies.
Exploits, Ransomware and Viruses are NOT inevitable.

If you need help...
Conclusion

Simplify your Layers and Reduce Your Costs with SECaaS (SECurity–as–a-Service)

*Includes the following layers in one solution:

*24/7 Network Security Monitoring and Reporting - knowledgeable professional security staff monitoring network traffic and remediating/reacting to threats as needed

*Hardware Firewall - configured with “Deny All” rules and then ports opened up only as needed

*Block TOR/I2P and other Ransomware specific apps/protocols

*Inspect SSL traffic using DPI-SSL

*Gateway Network Antivirus / AntiMalware - only catch 10%-40% of threats however still a mandatory first level of defense

*Internet Content Filter - must have for all Internet connected PCs.

*Advanced Monitoring - IPS, IDS, etc (Optional Sandbox)

*White Hat Social Engineering - test the effectiveness of your user's security awareness. Send “white hat” phishing emails to see which users need more limitations or training. The best firewall is the “human firewall”.

domain
computer services
Conclusion

Simplify your Layers and Reduce Your Costs with SECaaS (SECurity—as—a-Service)

*All plans include hardware firewall devices, software licenses, security service licenses and connection to our 24/7 NOC for alerting.

<table>
<thead>
<tr>
<th># of recommended max users supported</th>
<th>Fully Managed</th>
<th>Monitoring and Reporting</th>
<th>Basic Alerting</th>
<th>Install FM/MR/BA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-9</td>
<td>$139</td>
<td>$131</td>
<td>$86</td>
<td>Included/$500/$500</td>
</tr>
<tr>
<td>10-19</td>
<td>$220</td>
<td>$152</td>
<td>$107</td>
<td>Included/$500/$500</td>
</tr>
<tr>
<td>20-29</td>
<td>$250</td>
<td>$182</td>
<td>$137</td>
<td>Included/$500/$500</td>
</tr>
<tr>
<td>30-39</td>
<td>$279</td>
<td>$211</td>
<td>$165</td>
<td>Included/$500/$500</td>
</tr>
<tr>
<td>40-49</td>
<td>$322</td>
<td>$347</td>
<td>$237</td>
<td>Included/$750/$750</td>
</tr>
<tr>
<td>50-249</td>
<td>$646</td>
<td>$471</td>
<td>$361</td>
<td>Included/$750/$750</td>
</tr>
<tr>
<td>250-499</td>
<td>$771</td>
<td>$596</td>
<td>$486</td>
<td>Included/ Hourly/Hourly</td>
</tr>
<tr>
<td>500-1499</td>
<td>$2368</td>
<td>$1388</td>
<td>$943</td>
<td>Included/ Hourly/Hourly</td>
</tr>
<tr>
<td>1500-2999</td>
<td>$3055</td>
<td>$2075</td>
<td>$1630</td>
<td>Included/ Hourly/Hourly</td>
</tr>
</tbody>
</table>
Conclusion

Get Expert Compliance guidance and support with CISOaaS (CISO–as–a–Service)

Industry compliance regulations for cyber security are constantly changing. With CISO-as-a-Service, we’ll stay on top of it so you don’t have to.

- Access to a high-level IT security consultant.
- Information security policies and procedures to maintain compliance.
- Keep you updated on your environment and industry regulations.

Our CISO-as-a-Service (CISOaaS) Solution includes:

- Quarterly Security Audits
- Custom Security Policies & Procedures
- Industry Specific Security Compliance
- Ongoing Updates & Maintenance
- Cost Effective Security Consulting
Conclusion

Get Expert Compliance guidance and support with CISOaaS (CISO-as-a-Service)

Information Security Policies

A key component of a successful cyber security program to ensure your business maintains regulatory compliance for ISO27000, PCI DSS, and HIPAA/HITECH are effective policies and procedures designed for your business. With our CISOaaS, we provide the following policies, customized for your business to maintain compliance.

- Access Request Processing Policy
- Acceptable Use Policy
- Audit Controls Policy
- Authentication and Passwords Management Policy
- Breach Notification Policy
- Email Policy
- Encryption Policy
- Complaint Processing Policy
- Contingency Plan
- Cybersecurity Policy
- Device and Media Controls
- Facility Access Controls
- Firewall / DMZ Policy
- Information Disclosure Policy
- Marketing Policy
- Mobile Device Policy
- Malicious Software Controls Policy
- Privacy Notice Policy
- Remote Access Policy
- Router Security Policy
- Security Awareness and Training Policy
- Security Event Reporting Policy
- Server Security Policy
- Transmission Security Policy
- User Access Management Policy
- Workstation Security Policy
- Wireless Communications Policy
Notes

Cyber security breach Figures and tables courtesy of 2011/2012/2013/2014 Verizon Data Breach Investigations Report


Email:

rashaad@go-domain.com