IT SECURITY IN A WORLD OF RANSOMWARE ATTACKS

AGENDA

- Introductions
- What is Ransomware?
- Ransomware Risks
- What Can You Do
- Table Top Exercises
- Wrap Up

Privacy & Security

Ransomware attack on dermatology office breaches more than 13,000 patient records

The Reston, Virginia provider said patient protected health information and financial data was compromised by unauthorized third parties outside of the U.S.

By Jessica Davis | August 10, 2016 | 03:38 PM

SHARE 70

Healthcare orgs at much higher risk of ransomware attack than financial institutions

By Meg Bryant | July 28, 2016 print

Hacker posts 9.3M patient records for sale on dark net

By Meg Bryant | June 29, 2016 print

Privacy & Security

Ransomware: See the 8 hospitals already hit in 2016

By Jessica Davis | June 02, 2016 | 09:13 AM

SHARE 87

Privacy & Security

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By Bill Siwicki | May 23, 2016 | 02:58 PM

SHARE 810

Privacy & Security

Methodist Hospital recovering from five day ransomware attack, claims it did not pay up

Cybercriminals locked down enough of the Kentucky hospital's data that it was forced to declare an internal state of emergency. Now officials are saying they resolved the situation without giving into attackers' demands.

By Bernie Monegain | March 22, 2016 | 09:47 AM

SHARE 211

Privacy & Security

Ponemon: 89 percent of healthcare entities experienced data breaches

Half are caused by criminal cyber attacks, half by human error.

By Bill Siwicki | May 11, 2016 | 08:31 PM

SHARE 23

Privacy & Security

More than half of hospitals hit with ransomware in last 12 months

New research by Healthcare IT News and HIMSS Analytics found considerable uncertainty, questionable business continuity plans, and the need for more effective end-user education rampant in the industry.

By Tom Sullivan | April 07, 2016 | 07:52 AM

SHARE 575

Government & Policy

Hackers hit two more hospitals with ransomware

By Mike Miliard | April 04, 2016 | 11:09 AM

SHARE 1

MALICIOUS SOFTWARE

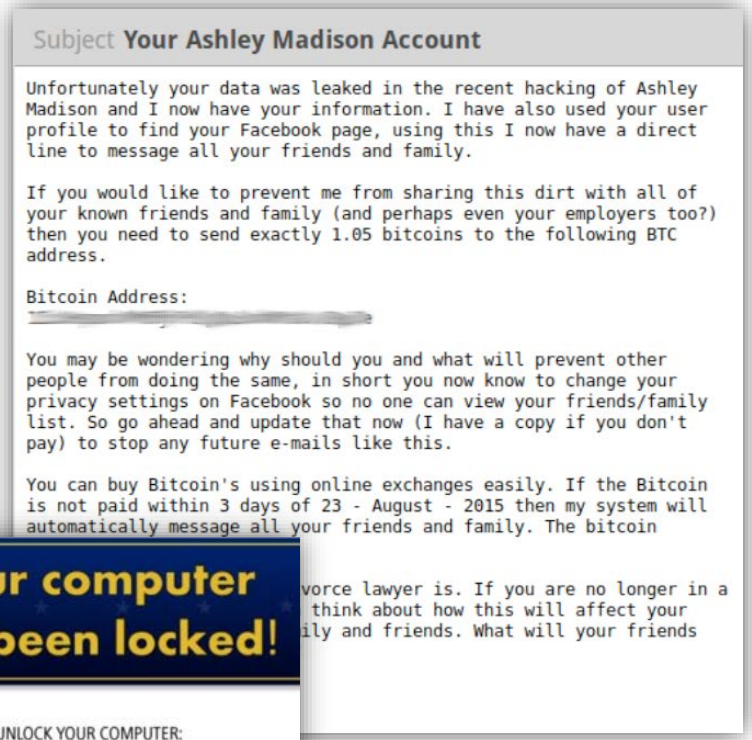
- Malware - malware refers to software programs designed to damage or do other unwanted actions on a computer system[1].
- Ransomware - is computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransom payment to restore it[2]

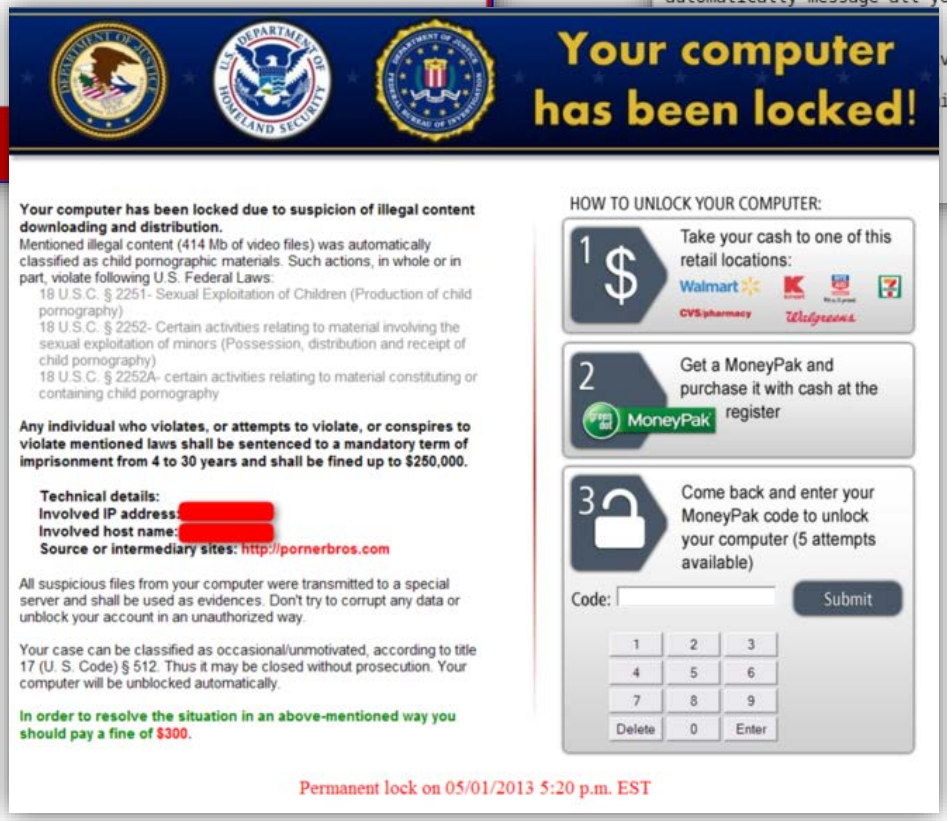
1. *http://techterms.com/definition/malware*
2. *https://en.wikipedia.org/wiki/Ransomware*

MALICIOUS SOFTWARE

- Denial of Service Attack / Distributed Denial of Service Attack (DoS / DDoS)
- Extortionware
- Spyware
- Scareware

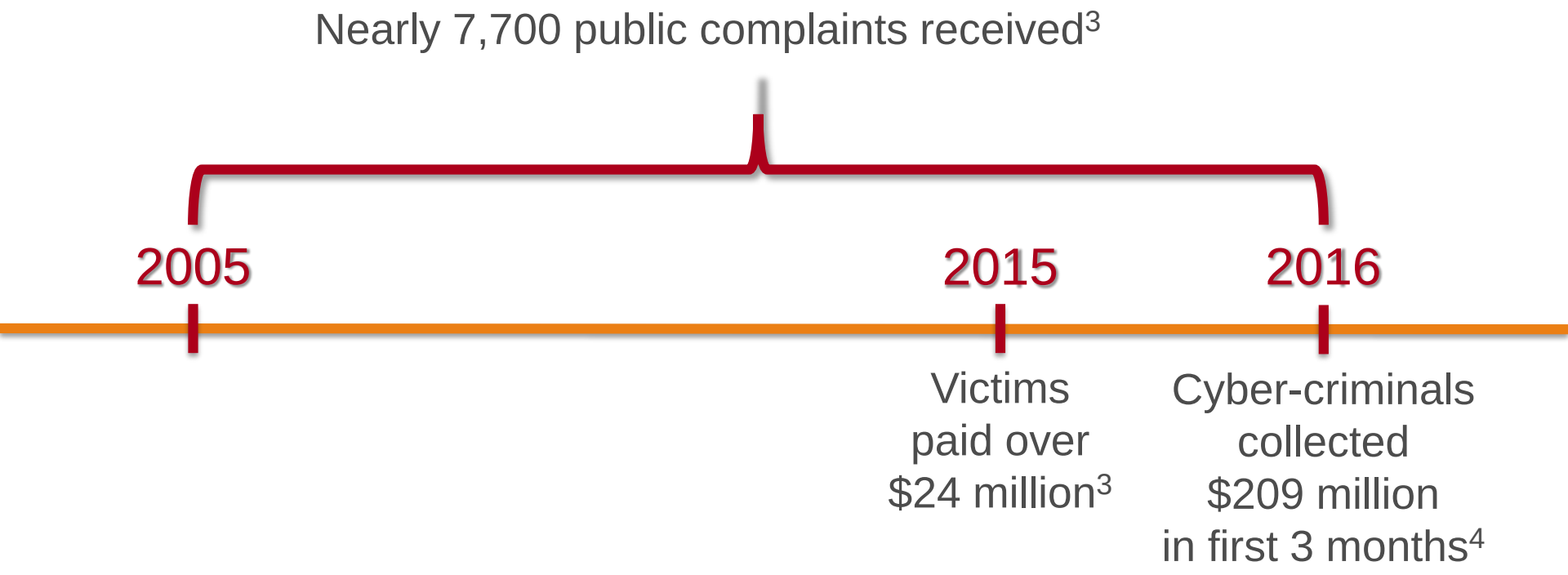

CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. 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.
Private key will be destroyed on
11/13/2013
1:27 AM
Time left
75 : 13 : 59


Subject Your Ashley Madison Account
Unfortunately your data was leaked in the recent hacking of Ashley Madison and I now have your information. I have also used your user profile to find your Facebook page, using this I now have a direct line to message all your friends and family.
If you would like to prevent me from sharing this dirt with all of your known friends and family (and perhaps even your employers too?) then you need to send exactly 1.05 bitcoins to the following BTC address.
Bitcoin Address:
You may be wondering why should you and what will prevent other people from doing the same, in short you now know to change your privacy settings on Facebook so no one can view your friends/family list. So go ahead and update that now (I have a copy if you don't pay) to stop any future e-mails like this.
You can buy Bitcoin's using online exchanges easily. If the Bitcoin is not paid within 3 days of 23 - August - 2015 then my system will automatically message all your friends and family. The bitcoin
vorce lawyer is. If you are no longer in a
think about how this will affect your
ily and friends. What will your friends


Your computer has been locked!
Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:
18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography
Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.
Technical details:
Involved IP address:
Involved host name:
Source or intermediary sites: http://pornerbros.com
All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.
Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.
In order to resolve the situation in an above-mentioned way you should pay a fine of $300.
HOW TO UNLOCK YOUR COMPUTER:
1 Take your cash to one of this retail locations:
Walmart
CVS/pharmacy
Walgreens
2 Get a MoneyPak and purchase it with cash at the register
MoneyPak
3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Code:
Submit
1 2 3
4 5 6
7 8 9
Delete 0 Enter
Permanent lock on 05/01/2013 5:20 p.m. EST

Why Is Ransomware Trending?

MONETIZATION OF RANSOMWARE

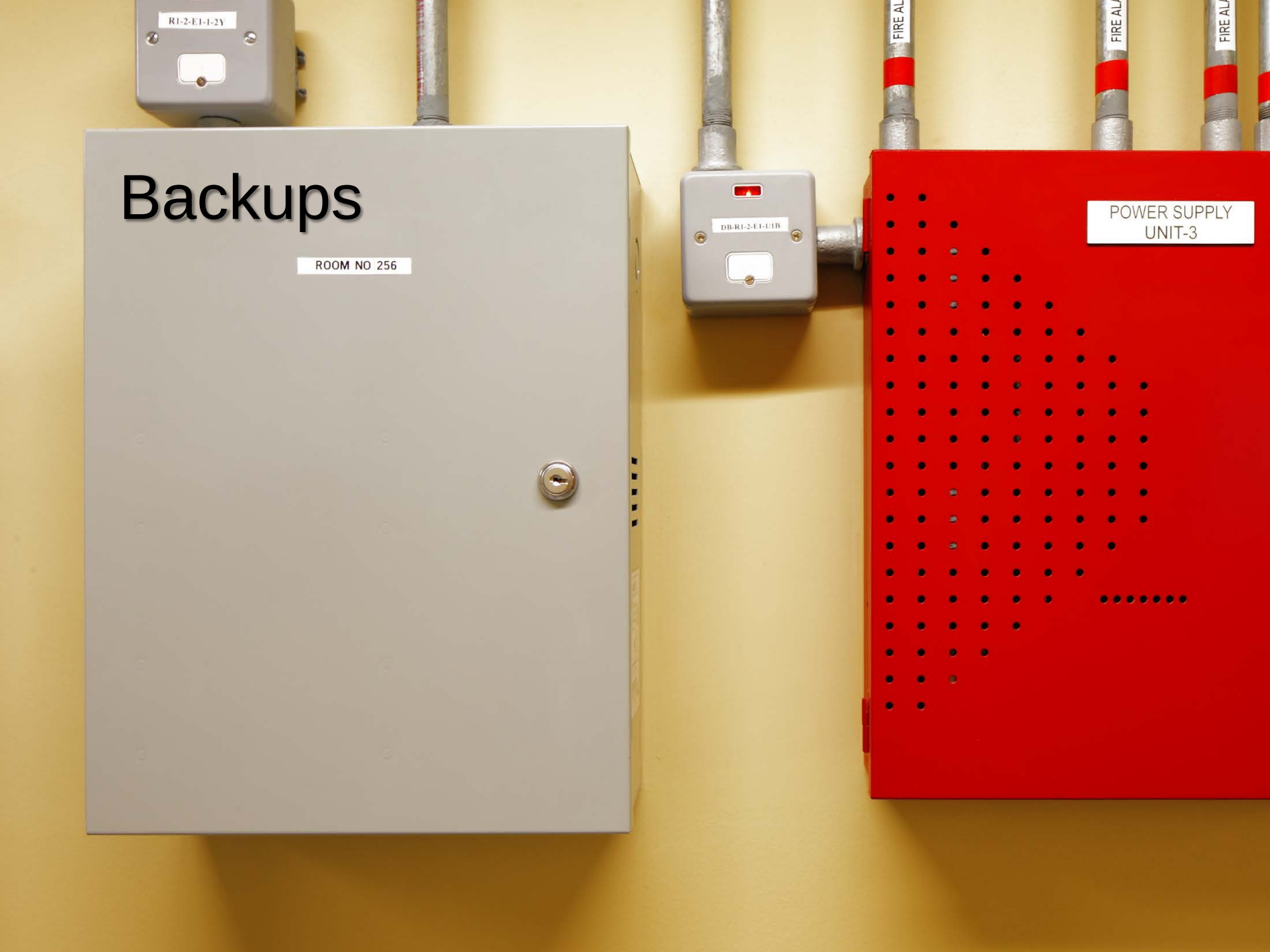


3. *http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4*
4. *http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/*

RANSOMWARE RISKS

- Your workforce
- Lack of awareness
- Phishing attacks
- Malvertizing
- Lacking adequate backups and disaster recovery

Ransomware Defenses

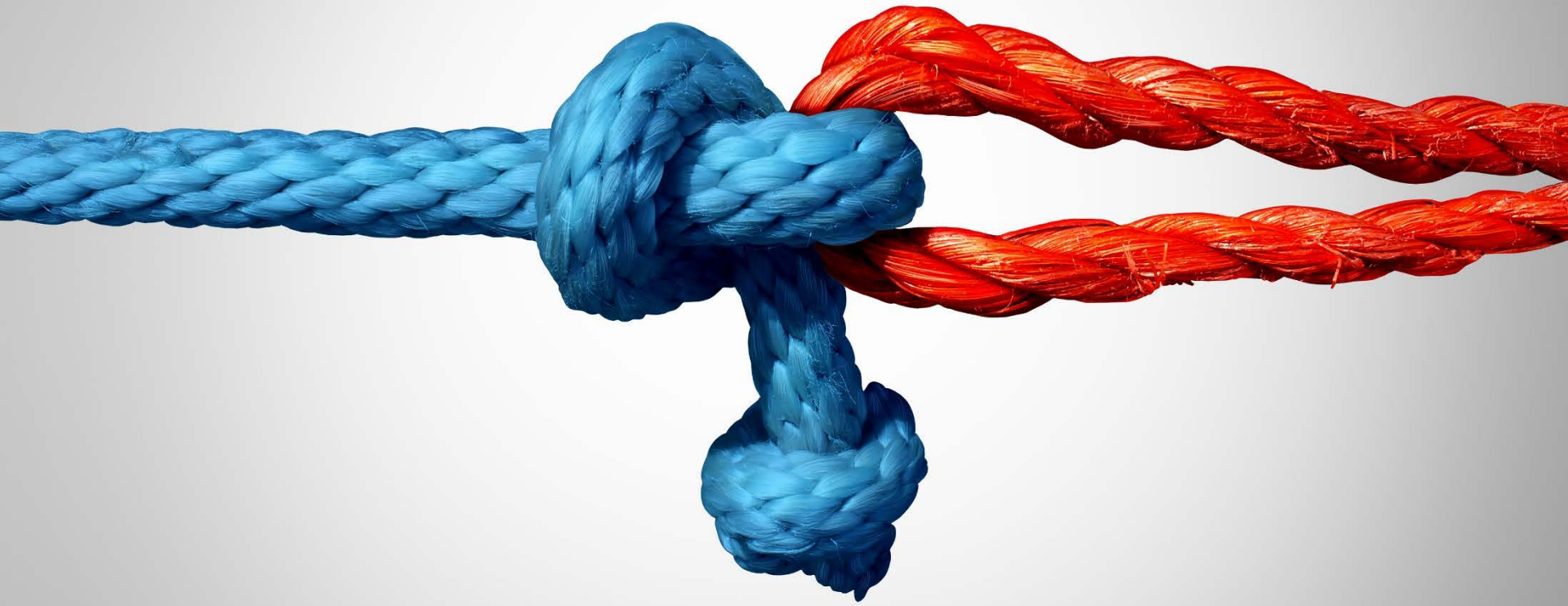

Backups
R1-2-E1-1-2Y
ROOM NO 256
DB-R1-2-E1-1/1B
POWER SUPPLY
UNIT-3


Patching

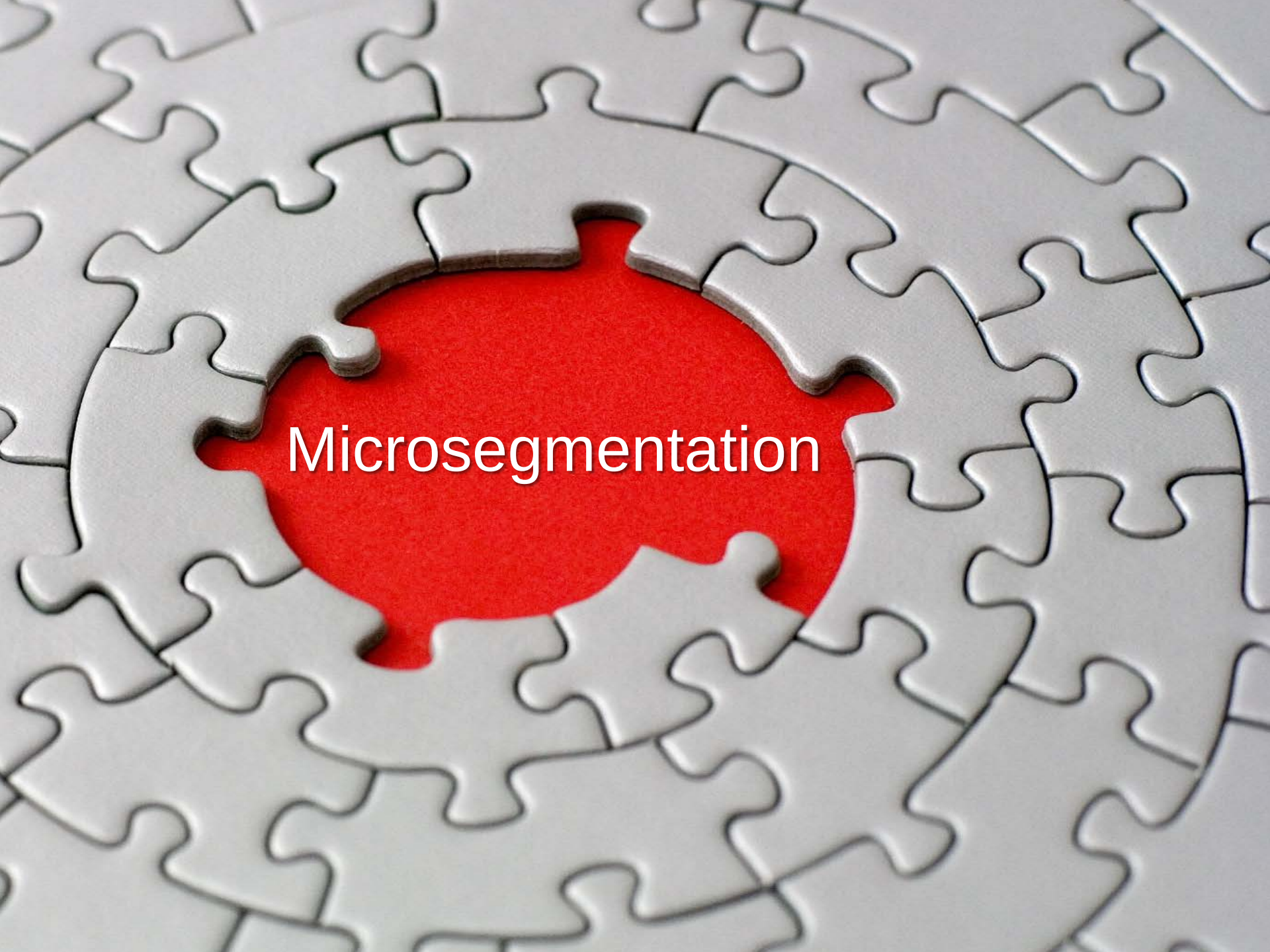
Antivirus Software

Disabling Administrative Access

Trusted Applications



Prevent Autoplay Capability


Microsegmentation

Email Restrictions

New and Emerging Detection Software

Workforce Education

Incident Response Plans

Practice: Table Top Exercise

QUESTIONS?

Dan Vogt

207.541.2279

dvogt@berrydunn.com