NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Healthcare Risks and Security Best Practices

Presentation for: HCCA™ Health Care Compliance Association

Advice
Strategy
Solutions
Consulting

Presenting Today

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

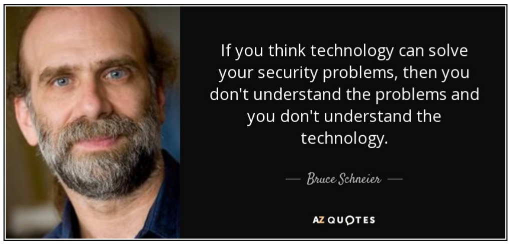
JEFF PEREIRA
Principal Consultant
Cell Phone: (646) 621-8050
Email: jpereira@nystec.com

http://www.nystec.com/
https://infosec.nystec.com/

2

Technology is the answer!

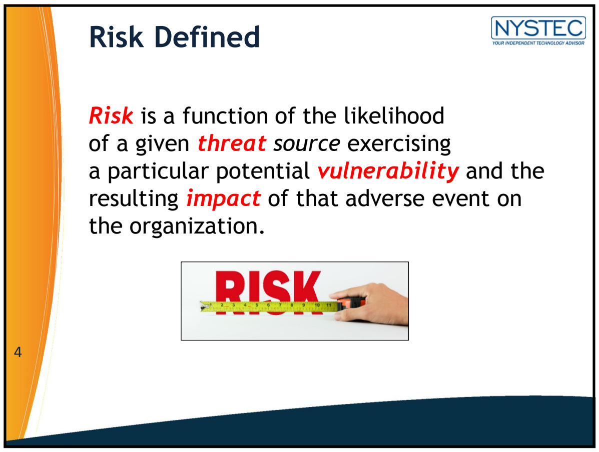
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR


If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— Bruce Schneier —

3

www.schneier.com

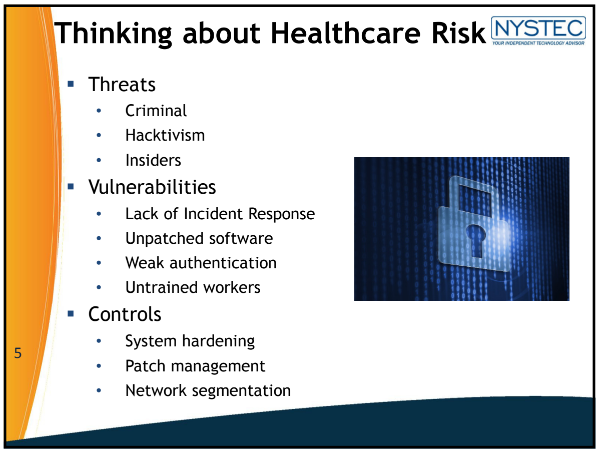


Risk Defined

NYSTEC

Risk is a function of the likelihood of a given ***threat*** *source* exercising a particular potential ***vulnerability*** and the resulting ***impact*** of that adverse event on the organization.

4

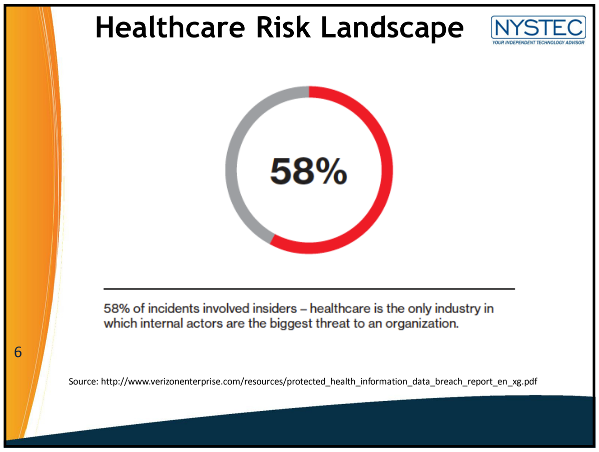


Thinking about Healthcare Risk

NYSTEC

- Threats
  - Criminal
  - Hacktivism
  - Insiders
- Vulnerabilities
  - Lack of Incident Response
  - Unpatched software
  - Weak authentication
  - Untrained workers
- Controls
  - System hardening
  - Patch management
  - Network segmentation

5



Healthcare Risk Landscape

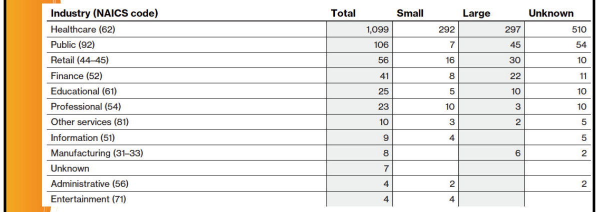
NYSTEC

58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.

6

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

Healthcare Risk Landscape



Industry (NAICS code)	Total	Small	Large	Unknown
Healthcare (62)	1,099	292	297	510
Public (92)	106	7	45	54
Retail (44–45)	56	16	30	10
Finance (52)	41	8	22	11
Educational (61)	25	5	10	10
Professional (54)	23	10	3	10
Other services (81)	10	3	2	5
Information (51)	9	4		5
Manufacturing (31–33)	8		6	2
Unknown	7			
Administrative (56)	4	2		2
Entertainment (71)	4	4		

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

The Actors

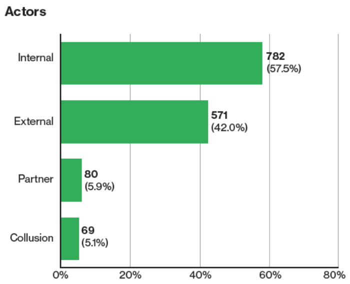


Figure 1. Threat actors within PHIDBR dataset, n=1,360

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

The Actions

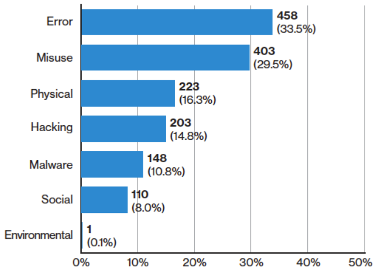


Figure 2. Threat action categories within PHIDBR dataset, n=1,368

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

The Hacks

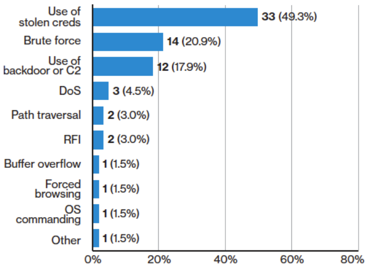


Figure 6. Threat action varieties within Hacking, n=67

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

10

The Malware

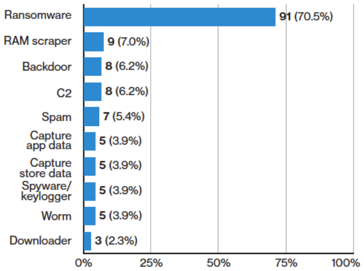
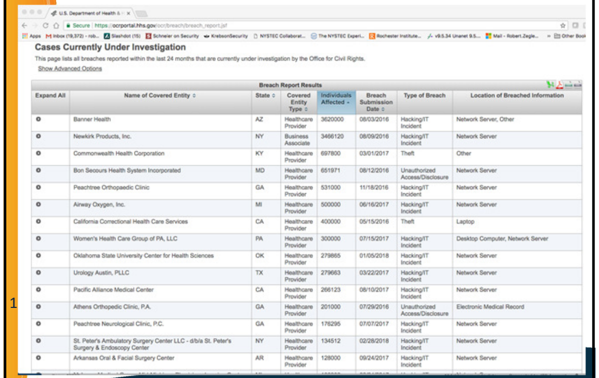


Figure 7. Threat action varieties within Malware, n=129

Source: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

11

The Results?



Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

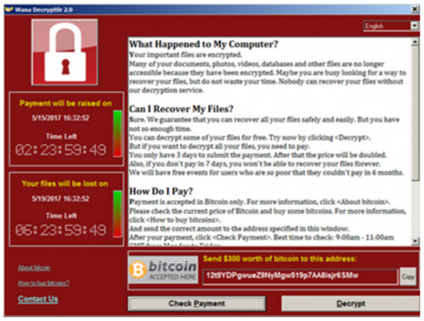
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
⊕	Banner Health	AZ	Healthcare Provider	3620000	08/03/2016	Hacking/IT Incident	Network Server, Other
⊕	Newkirk Products, Inc.	NY	Business Associate	3466120	08/09/2016	Hacking/IT Incident	Network Server
⊕	Commonwealth Health Corporation	KY	Healthcare Provider	697800	03/01/2017	Theft	Other
⊕	Bon Secours Health System Incorporated	MD	Healthcare Provider	651971	08/12/2016	Unauthorized Access/Disclosure	Network Server
⊕	Peachtree Orthopaedic Clinic	GA	Healthcare Provider	531000	11/18/2016	Hacking/IT Incident	Network Server
⊕	Airway Oxygen, Inc.	MI	Healthcare Provider	500000	06/16/2017	Hacking/IT Incident	Network Server
⊕	California Correctional Health Care Services	CA	Healthcare Provider	400000	05/15/2016	Theft	Laptop
⊕	Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300000	07/15/2017	Hacking/IT Incident	Desktop Computer, Network Server
⊕	Oklahoma State University Center for Health Sciences	OK	Healthcare Provider	279865	01/05/2018	Hacking/IT Incident	Network Server
⊕	Urology Austin, PLLC	TX	Healthcare Provider	279663	03/22/2017	Hacking/IT Incident	Network Server
⊕	Pacific Alliance Medical Center	CA	Healthcare Provider	266123	08/10/2017	Hacking/IT Incident	Network Server
⊕	Athens Orthopedic Clinic, P.A.	GA	Healthcare Provider	201000	07/29/2016	Unauthorized Access/Disclosure	Electronic Medical Record
⊕	Peachtree Neurological Clinic, P.C.	GA	Healthcare Provider	176295	07/07/2017	Hacking/IT Incident	Network Server
⊕	St. Peter's Ambulatory Surgery Center LLC - d/b/a St. Peter's Surgery & Endoscopy Center	NY	Healthcare Provider	134512	02/28/2018	Hacking/IT Incident	Network Server
⊕	Arkansas Oral & Facial Surgery Center	AR	Healthcare Provider	128000	09/24/2017	Hacking/IT Incident	Network Server

1

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Threats

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

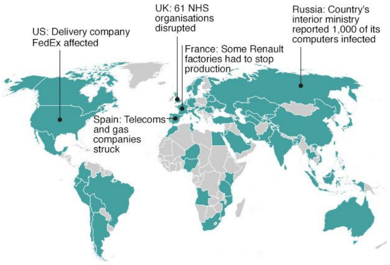
13

Source: krebsonsecurity.com

Threats

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR

Countries hit in initial hours of cyber-attack



UK: 61 NHS organisations disrupted
Russia: Country's interior ministry reported 1,000 of its computers infected
US: Delivery company FedEx affected
France: Some Renault factories had to stop production
Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team BBC

14

Threats

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR

Allscripts

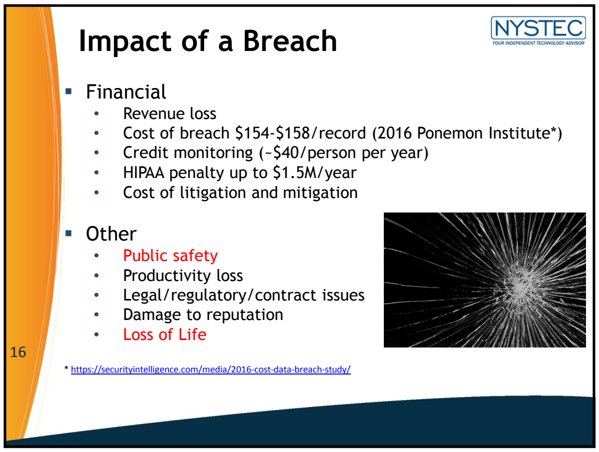
A surgical center affiliated with St. Peter's Hospital has been hit by the second-largest computer breach of patient records in New York state since 2016. Timesunion.com

Anthem.

mongoDB

Sheriffs warn of hackers after upstate attack
Thedailystar.com

15

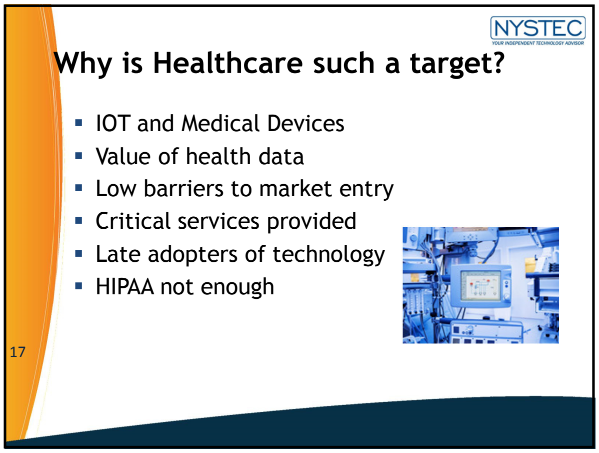


Impact of a Breach

- Financial
  - Revenue loss
  - Cost of breach $154-$158/record (2016 Ponemon Institute*)
  - Credit monitoring (~$40/person per year)
  - HIPAA penalty up to $1.5M/year
  - Cost of litigation and mitigation
- Other
  - Public safety
  - Productivity loss
  - Legal/regulatory/contract issues
  - Damage to reputation
  - Loss of Life

16

* https://securityintelligence.com/media/2016-cost-data-breach-study/



Why is Healthcare such a target?

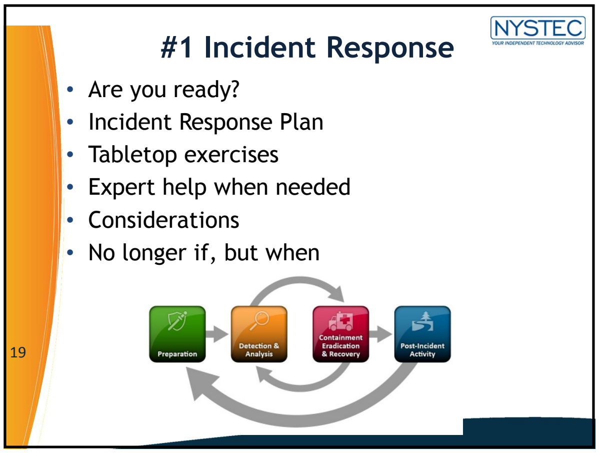
- IOT and Medical Devices
- Value of health data
- Low barriers to market entry
- Critical services provided
- Late adopters of technology
- HIPAA not enough

17

Healthcare Security

Best Practices

18

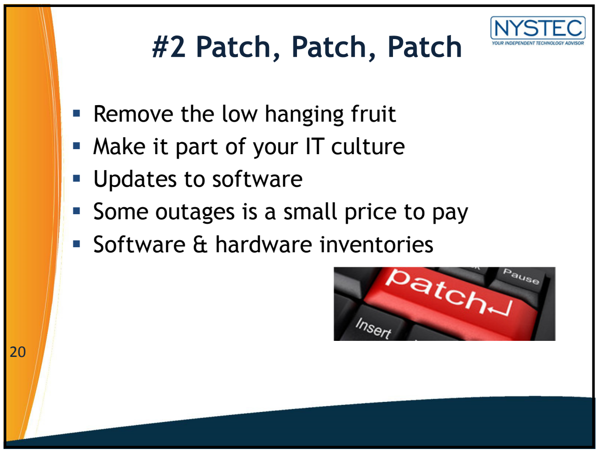


#1 Incident Response

- Are you ready?
- Incident Response Plan
- Tabletop exercises
- Expert help when needed
- Considerations
- No longer if, but when

Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

19

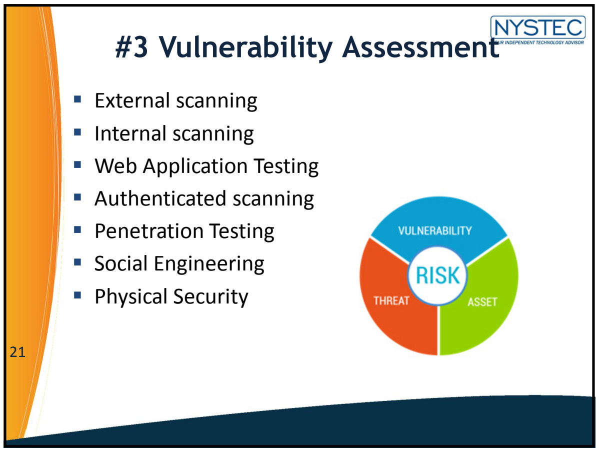


#2 Patch, Patch, Patch

- Remove the low hanging fruit
- Make it part of your IT culture
- Updates to software
- Some outages is a small price to pay
- Software & hardware inventories

patch
Pause
Insert

20

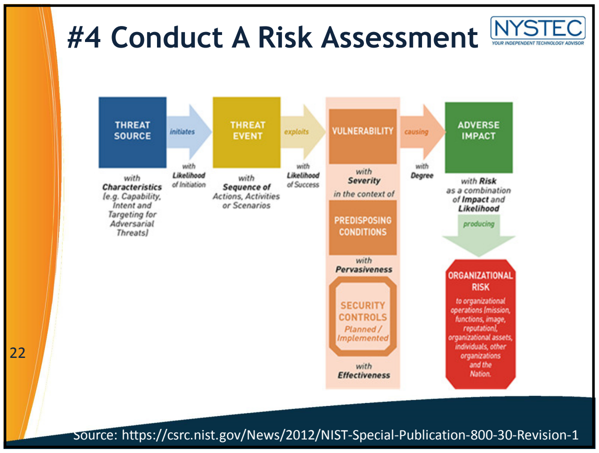


#3 Vulnerability Assessment

- External scanning
- Internal scanning
- Web Application Testing
- Authenticated scanning
- Penetration Testing
- Social Engineering
- Physical Security

VULNERABILITY
RISK
THREAT
ASSET

21



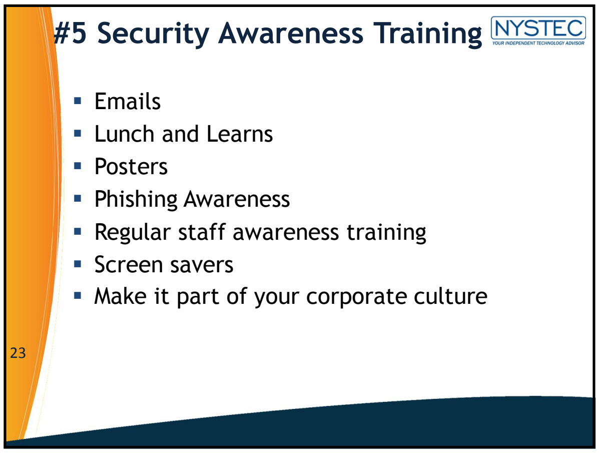
#4 Conduct A Risk Assessment

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR

THREAT SOURCE
initiates
with Likelihood of Initiation
with Characteristics (e.g. Capability, Intent and Targeting for Adversarial Threats)
THREAT EVENT
exploits
with Likelihood of Success
with Sequence of Actions, Activities or Scenarios
VULNERABILITY
with Severity
in the context of
PREDISPOSING CONDITIONS
with Pervasiveness
SECURITY CONTROLS Planned / Implemented
with Effectiveness
causing
with Degree
ADVERSE IMPACT
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
to organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations and the Nation.

22

Source: https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1

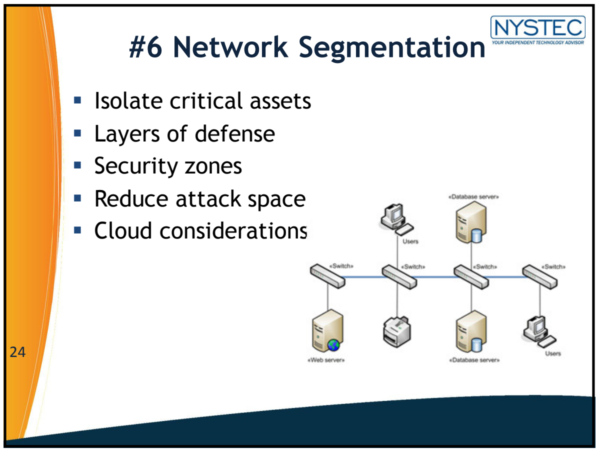


#5 Security Awareness Training

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR

- Emails
- Lunch and Learns
- Posters
- Phishing Awareness
- Regular staff awareness training
- Screen savers
- Make it part of your corporate culture

23

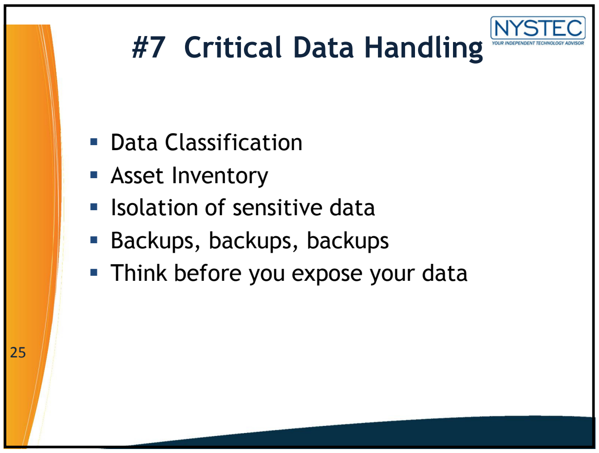


#6 Network Segmentation

NYSTEC YOUR INDEPENDENT TECHNOLOGY ADVISOR

- Isolate critical assets
- Layers of defense
- Security zones
- Reduce attack space
- Cloud considerations

24

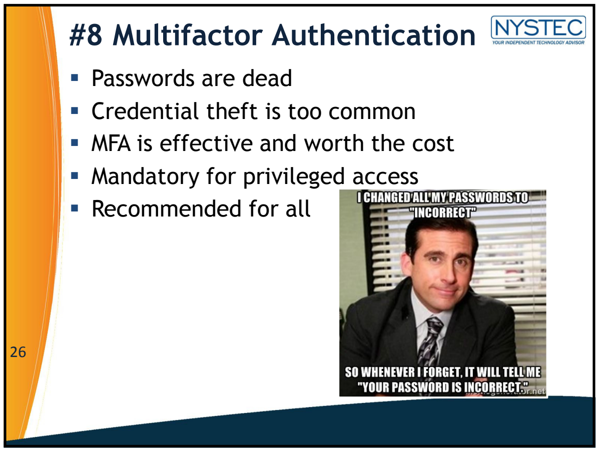


#7 Critical Data Handling

NYSTEC

- Data Classification
- Asset Inventory
- Isolation of sensitive data
- Backups, backups, backups
- Think before you expose your data

25



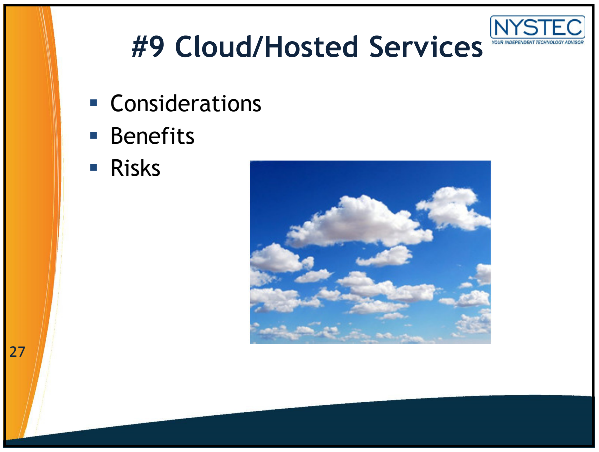
#8 Multifactor Authentication

NYSTEC

- Passwords are dead
- Credential theft is too common
- MFA is effective and worth the cost
- Mandatory for privileged access
- Recommended for all

I CHANGED ALL MY PASSWORDS TO "INCORRECT"
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."

26



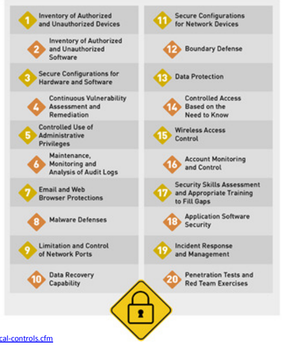
#9 Cloud/Hosted Services

NYSTEC

- Considerations
- Benefits
- Risks

27

#10 Align with CIS Top 20*



1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

* https://www.cisecurity.org/critical-controls.cfm

28

Security is a Process. Built In, Not Bolted On.

29

Questions

30