BerryDunn

WV HFMA FALL INSTITUTE 2017

HIPAA Security Update

Presented By
Dan Vogt

September 29, 2017

Dan Vogt

Senior Manager in Management and IT Consulting Practice

Certified Professional in Electronic Health Records (CPEHR)

Certified Professional in Healthcare Management and Information Systems (CPHIMS)

Project Management Professional (PMP)

HIMSS Advocate

Lehigh University Alumni

Dad of a 4 year old daughter and 18 month old son

Goal

To gain perspective on HIPAA Security in context with current risks.

Current Situation

- Security Rule is almost 15 years old
- Meaningful Use is 7 years old
- EHR adoption is increasing
- OCR is conducting HIPAA audits
- Ransomware incidents are increasing

Agenda

1 CURRENT EVENTS AND CONTEXT

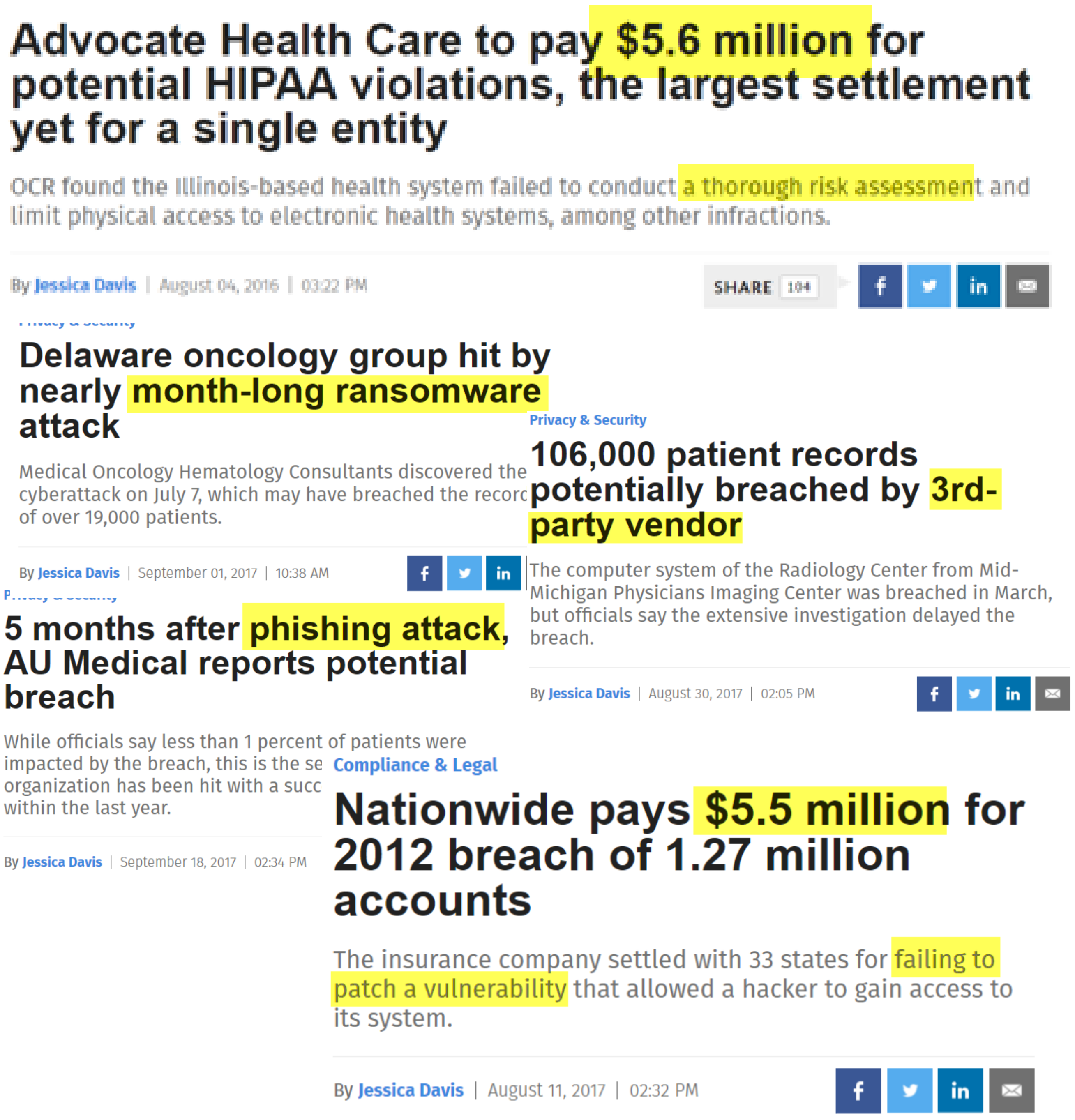
2 PERSPECTIVE ON SECURITY RULE

3 TEN TECHNOLOGY RISKS

Audience Benefits

- Understanding of the Security Rule in current times
- Awareness of the OCR audits
- Greater appreciation for risk analysis
- Identification of potential risks

In the News



Advocate Health Care to pay $5.6 million for potential HIPAA violations, the largest settlement yet for a single entity

OCR found the Illinois-based health system failed to conduct a thorough risk assessment and limit physical access to electronic health systems, among other infractions.

By Jessica Davis | August 04, 2016 | 03:22 PM

Privacy & Security

Delaware oncology group hit by nearly month-long ransomware attack

Medical Oncology Hematology Consultants discovered the cyberattack on July 7, which may have breached the recorc of over 19,000 patients.

By Jessica Davis | September 01, 2017 | 10:38 AM

Privacy & Security

106,000 patient records potentially breached by 3rd-party vendor

The computer system of the Radiology Center from Mid-Michigan Physicians Imaging Center was breached in March, but officials say the extensive investigation delayed the breach.

By Jessica Davis | August 30, 2017 | 02:05 PM

Privacy & Security

5 months after phishing attack, AU Medical reports potential breach

While officials say less than 1 percent of patients were impacted by the breach, this is the se organization has been hit with a succ within the last year.

By Jessica Davis | September 18, 2017 | 02:34 PM

Compliance & Legal

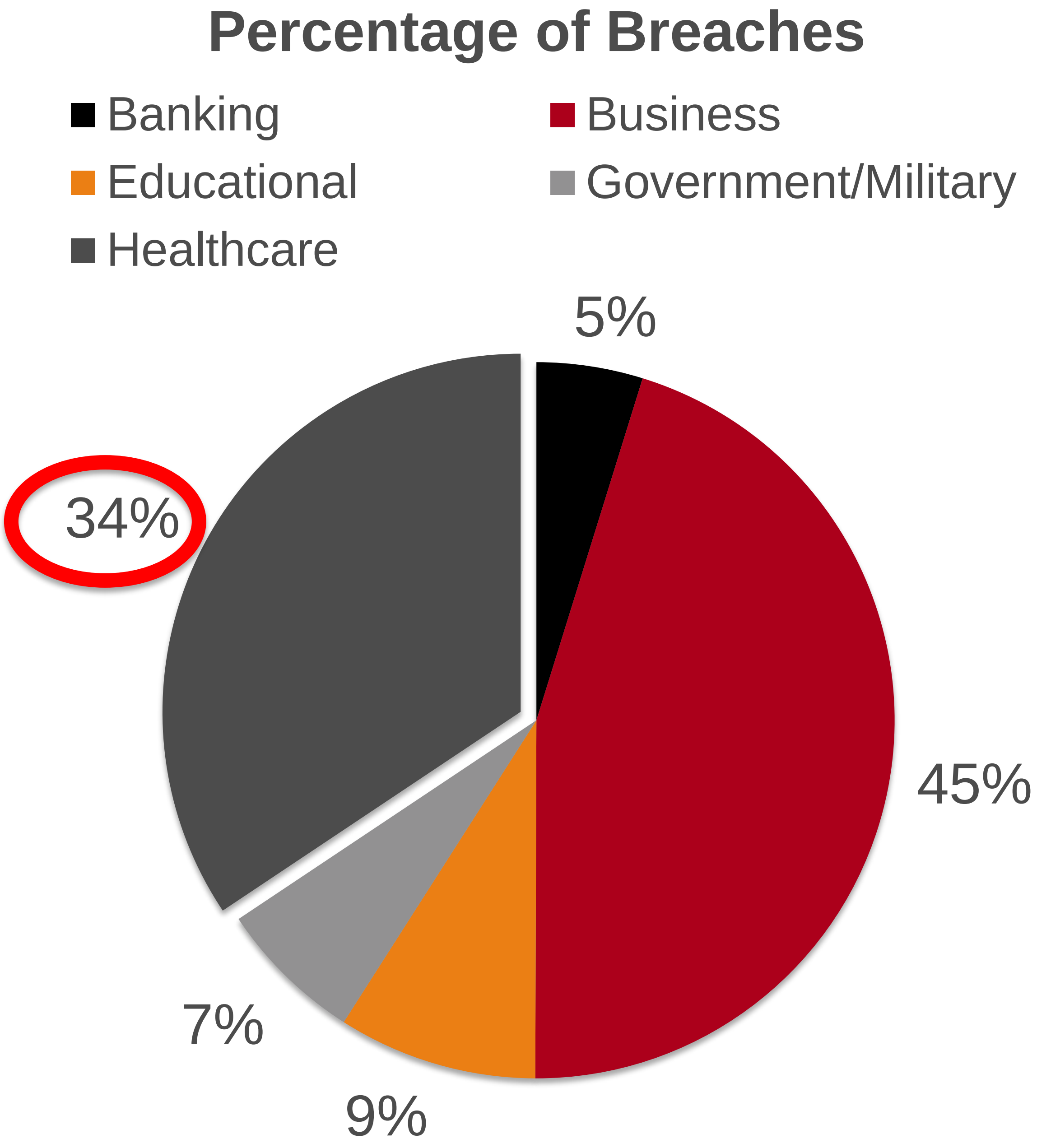
Nationwide pays $5.5 million for 2012 breach of 1.27 million accounts

The insurance company settled with 33 states for failing to patch a vulnerability that allowed a hacker to gain access to its system.

By Jessica Davis | August 11, 2017 | 02:32 PM

Breaches

SOURCES



http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

Breaches

COST

Average[1]

$225 per record

Healthcare[1]

$380 per record

1. Ponemon Institute – 2017 Cost of Data Breach Study

OCR

HIPAA AUDITS

- OCR has completed over 200 desk audits
- Onsite audits begin in 2017 – 2018

OCR FINDINGS THUS FAR:

- Risk analysis
- Risk management
- Business associate agreements
- Transmission security
- Auditing
- Software patching
- Media disposal
- Backup and contingency planning

Administrative Safeguards

Standard	Implementation Specification	R/A
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assign Security Responsibility		R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A

Administrative Safeguards (cont.)

Standard	Implementation Specification	R/A
Information Access Management	Isolating Health Care Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness and Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A
Security Incident Procedures	Response and Reporting	R

Administrative Safeguards (cont.)

Standard	Implementation Specification	R/A
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedures	A
	Application and Data Criticality Analysis	A
Evaluation		R
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	R

Physical Safeguards

Standard	Implementation Specification	R/A
Facility Access Controls	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A
Workstation Use		R
Workstation Security		R
Device and Media Controls	Disposal	R
	Media Re-Use	R
	Accountability	A
	Data Backup and Storage	A

Technical Safeguards

Standard	Implementation Specification	R/A
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls		R
Integrity	Mechanism to Authenticate Electronic PHI	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

#1

THE INTERNET OF THINGS (IoT)

WHAT CAN YOU DO?

- Change your password and other settings where possible
- Turn it off when not in use
- Update and re-boot at least weekly
- Conduct a risk assessment specific to devices
- Monitor your network for suspicious activity
- Consider separate and secure network for devices.

#2

NETWORK SECURED ONLY AT PERIMETER

#2

NETWORK SECURED ONLY AT PERIMETER

WHAT CAN YOU DO?

- Multiple firewalls should be in place throughout network
- Segmentation – break servers apart by function with strong access rules
- Monitor network traffic throughout systems
- Segregation of Duties – much like accounting roles
- Log review and alerting

#3

THE WORLD OF FAKES

#3

THE WORLD OF FAKES

WHAT CAN YOU DO?

Understand the source and think about the context

- Validate through multiple sources of information
- Run your anti-virus software before you click
- Don’t “friend” unknown people
- Set Google alerts for your Organization
- Have a PR plan ready
- Build into workforce training

#4

SMARTPHONE HACKING

LOST OR STOLEN PHONES

In the last 3 years it is estimated that 2.1 to 3.3 million phones are lost or stolen in the US each year

72% **American's own a smart phone**

4.5% **Company's mobile assets are lost or stolen each year**

THOSE NUMBERS COMBINED WITH -

Users' continued insistence on merging personal device for work information

30 TO **35%** **Smart phone owners do not use a passcode to access their phone**

#4

SMARTPHONE HACKING

WHAT CAN YOU DO?

- Use a passcode!
- Avoid clicking on short links (used on social media most often)
- Only purchase/download applications from the iTunes or Android store
- Train employees on phishing attempts
- Use a container application for work email and data
- Maintain ability to wipe employees’ lost or stolen phones

#5

MERGERS & ACQUISITIONS

#5

MERGERS & ACQUISITIONS

WHAT CAN YOU DO?

- Understand systems of both organizations
- Take inventory of systems, data, and hardware
- Undertake an M&A IT Risk Assessment
- Test systems extensively
- Understand roles and personnel
- Phase in the merger
- Continuous verification and data integrity checks
- Add protection layers between environments

#6

GOVERNMENT HACKING

#6

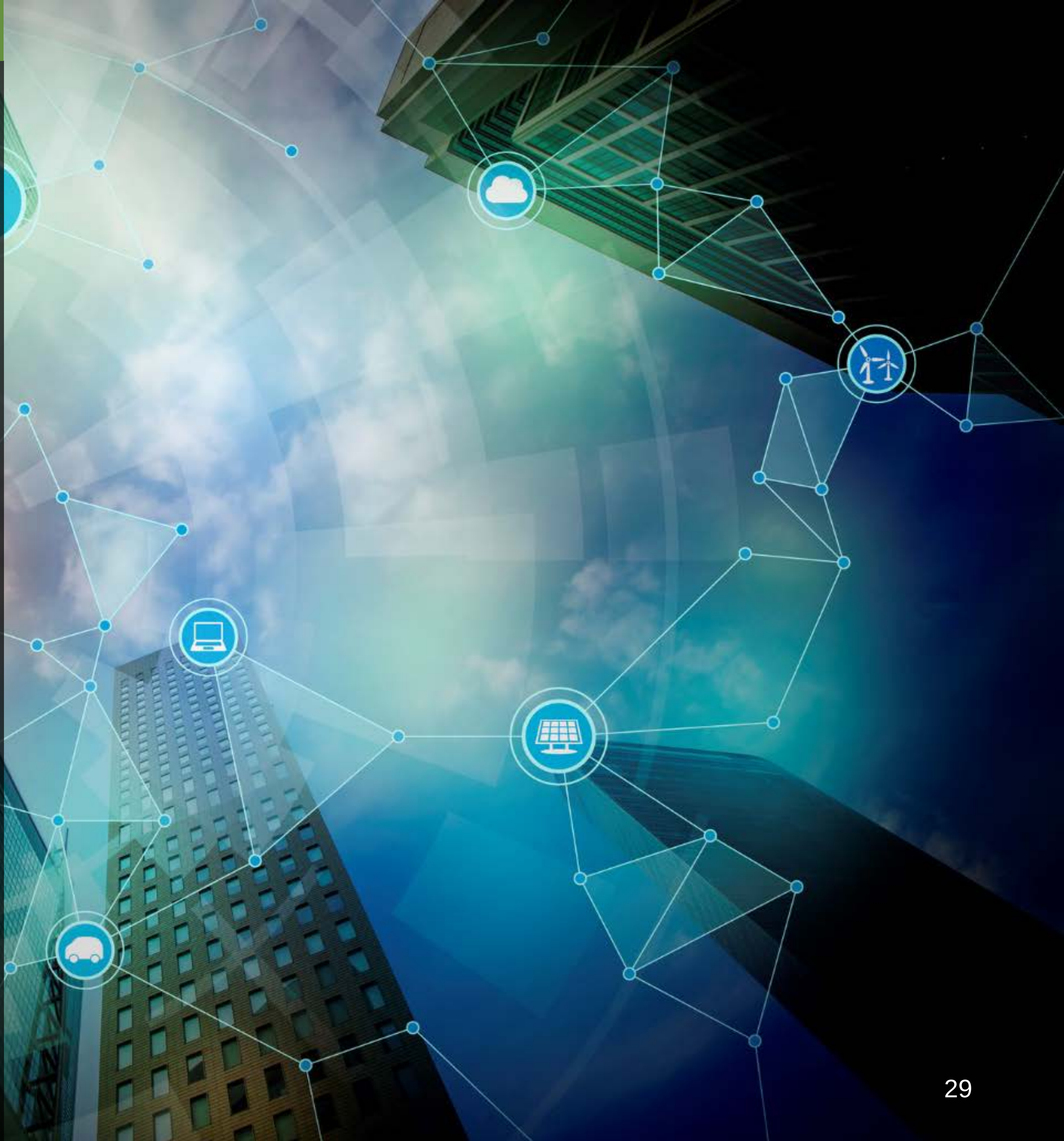
GOVERNMENT HACKING

WHAT CAN YOU DO?

- Employee background checks
- Manage access – rule of least privilege
- Know what data you have and where it is
- Monitor internal activity
- Prevent local saving – data grabbing
- Don’t ignore patches – often these are addressing 0-day vulnerabilities
- Force Weekly server re-boots
- Firewalls and Intrusion Detection Systems should be in place

#7

CYBER INSURANCE



#7

CYBER INSURANCE

WHAT CAN YOU DO?

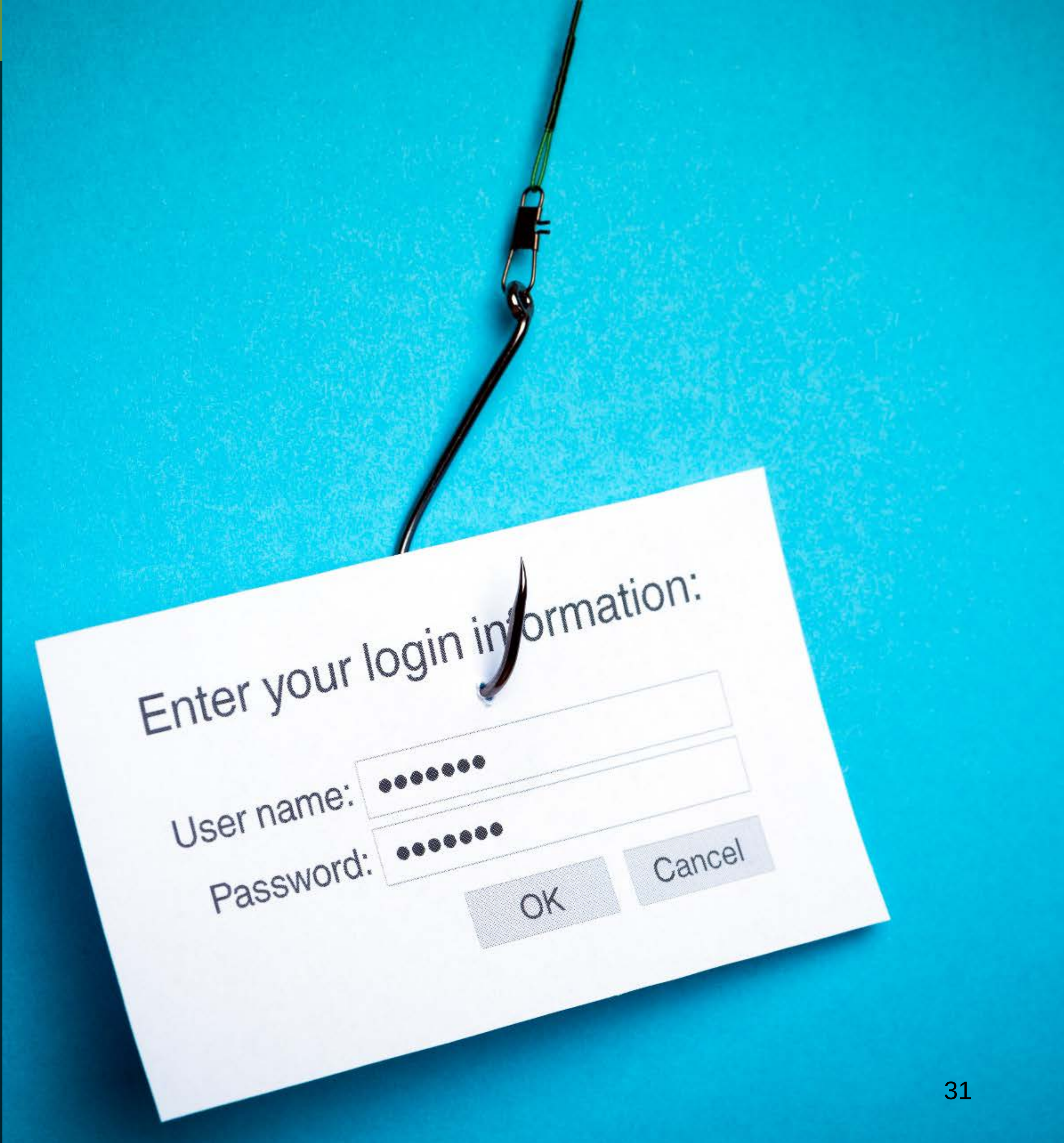
- Cyber Insurance is used as a last resource
- Critical to have, but you should have a robust security program in place as well
- Backups and Business Continuity

THINGS TO CONSIDER…

1. May not cover your reputation
2. Expensive for good coverage
3. Effective if you have the right coverage

#8

ADVANCED PHISHING SCAMS



#8

ADVANCED PHISHING SCAMS

WHAT CAN YOU DO?

Always be a skeptic.

- If it looks fake, it is fake. Call the company, your helpdesk, etc.
- Companies do not email customers over account information
- Hover over the link….
- Security Awareness Training
- Social Engineering Testing
- Email filers, anti-virus, patching

#9

LACK OF IT SECURITY RISK ASSESSMENTS

#9

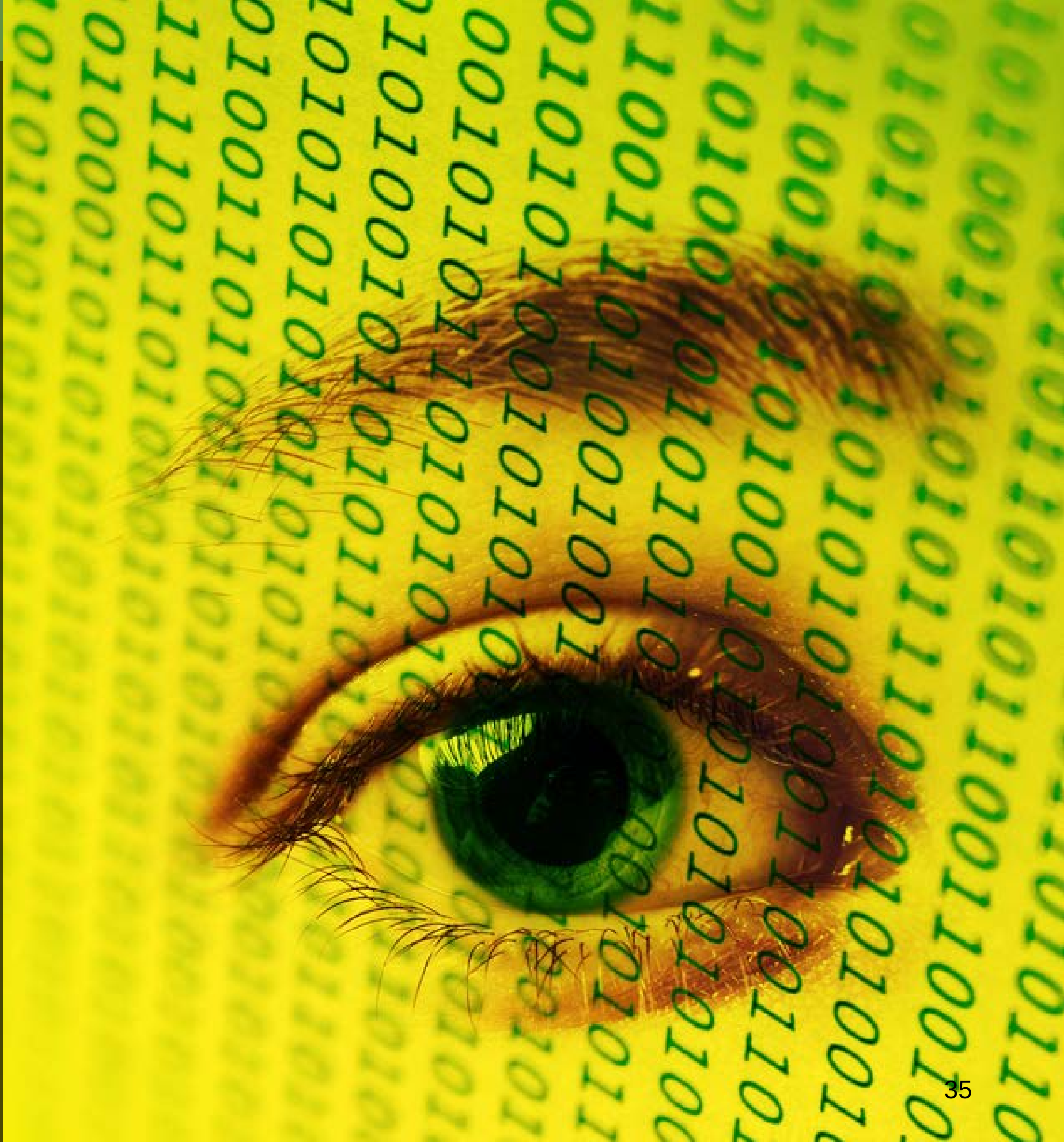
LACK OF IT SECURITY RISK ASSESSMENTS

WHAT CAN YOU DO?

- Risk Management Program
- Risk = Impact x Likelihood to occur
- You cannot secure your systems properly if you do not know where the potential gaps may be
- Pick a framework – CoBit, COSO, NIST
- Re-visit at least annually
- Make risk management a effort at the senior leadership and board level

#10

ADVANCED RANSOMWARE



#10

ADVANCED RANSOMWARE

WHAT CAN YOU DO?

- Employee training – STOP CLICKING!
- Take away local administrator use of employee workstations – prevents installation of software
- Backups and patches
- Disaster recovery planning
- Software whitelisting
- Disable auto-play
- Micro-segmentation
- Table top exercises
- Email filtering

Contact Us

DAN VOGT

Senior Manager
dvogt@berrydunn.com