



BerryDunn

Managing IT Risk: What Now and What to Look For

Presented By

Tina Bode | IT Assurance Services



Agenda

1 TOP TEN IT
SECURITY RISKS

2 WHAT YOU CAN DO

3 QUESTIONS

Introduction

IT'S ALL CONNECTED

All of our Top 10 risks impact us both as consumers and as professionals.

THE RISKS

- Created from input from all areas of our Firm
- Based on what we see every day
- From a blend of healthcare, private sector, governmental, and higher education industries

WHAT WE'LL LEARN TODAY....

- Overview of the risks
- The potential impact to you and your organization
- Suggestions for mitigating the risks



#1

THE INTERNET OF THINGS (IoT)

THE IoT

Any device that connects directly or indirectly through a Bluetooth connection, to a mothership device, and to the internet

ON A CONSUMER LEVEL

Amazon Echo, Google Home, Home security systems, your iWatch and fitness trackers

IN BUSINESS

Conference room systems, healthcare monitoring tools, printing presses, and surveillance systems

LIFE IS EASIER, BUT THERE IS RISK....

#1

THE INTERNET OF THINGS (IoT)

WHAT'S THE RISK?

Symantec estimates that in 2016, nearly 6.4 billion IoT devices around the world connected to the internet and that there were 25 IoT devices per 100 inhabitants in the US.

- Devices come shipped ready for “plug and play”
- Default Settings – sure it works, but it does for everyone else too
- Connected to your network and the Internet

HACKERS CAN EASILY “HIJACK THE DEVICE” IF DEFAULT SETTINGS ARE NOT CHANGED. THINK OF THE IMPACT....



#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
- Monitor your network for suspicious activity
- Separate and secure wireless networks for devices



#2

NETWORK SECURED ONLY AT PERIMETER

IT USED TO BE JUST ABOUT THE FRONT DOOR

- Firewalls at the point of your network and the Internet were sufficient protection
 - Multiple access points now should adjust that thinking
 - Threats from the inside
 - Your data is not just on your network now
- 

#2

NETWORK SECURED ONLY AT PERIMETER

FIREWALLS

Multiple firewalls should be in place throughout network

SERVERS

Segmentation – break servers apart by function with strong access rules

DUTIES

Segregation of duties – much like accounting roles

TRAFFIC

Monitor network traffic throughout systems

ALERTS

Log review and alerting



#3

THE WORLD OF FAKES

NOT ENTIRELY WHAT YOU ARE THINKING....

- Fake information that gets you to act or click
- Fake ransomware/virus notifications
- Fake helpdesk tickets or calls
- News alerts or order shipment
- Social Media accounts

#3

THE WORLD OF FAKES

WHAT CAN YOU DO?

Understand the source and think about the context

- Validate information through multiple sources
- Run your antivirus software before you click
- Hover before you click
- Don't "friend" unknown people
- Set Google alerts for your Organization
- Have a PR plan ready



#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%

Americans 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

A COMBINATION OF RISKS

PHISHING TEXTS – text messages seeking to deceit or trick a user



SICK APPLICATIONS

- **SCARE-WARE SOFTWARE** – fake threats that they found illegal material on phone – pay us now to fix it!
- **SNIFFING SOFTWARE** – software that steals data, such as account information for online banking
- **SPAM-BOTS** – software that takes over your social media accounts and spams contacts

#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 – banks will never text you for account information
- Use a container application for work email and data
- Maintain ability to wipe employee's phone's who are lost or stolen

#5

MERGERS & ACQUISITIONS

BIGGER IS NOT ALWAYS BETTER

- Big issue in healthcare – merging systems (ERP systems)
- Focus on operations/patient services and not on systems
- Personnel and Management changes that cause confusion and conflict
- Lack of testing for integration
- Two sets (or more) of data

75% OF MERGERS AND ACQUISITIONS FAIL DUE TO UNSUCCESSFUL SOFTWARE SYSTEM INTEGRATION

#5

MERGERS & ACQUISITIONS

WHAT CAN YOU DO?

SLOW DOWN!

- Understand systems of both organizations – which system will become the “master” or is a new system needed?
- Take inventory of systems, data, and hardware
- Test systems extensively before merging
- Understand roles and perform user reviews

BACK IT UP!

- Run systems in parallel until you are confident the merged system works
- Phase in the merger – department by department approach
- Continuous verification and data integrity checks



#6

GOVERNMENT HACKING

THIS IS NOT A NEW CONCEPT...

- Includes what we see in the news with attempts to influence political direction and results of elections
- New kind of a war – through technology we can cripple infrastructure and supply chains

MORE THAN POLITICS...

- 0-day vulnerabilities known by governments but kept secret
- Those vulnerabilities also impact industry as they are holes in systems and software

#6

GOVERNMENT HACKING

WHAT CAN YOU DO?

REDUCE DATA LEAKS AND BREACHES

- 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

PATCH!

- 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

TRANSFER OF RISK

Used in conjunction with risk management – transfer of risk – but there is over reliance

COSTS

Helps with costs of data breach, hacking, reputation loss, and remediation

RESPONSIBILITY

Data security is still your responsibility

KEY CONCEPT

The key concept for cyber insurance is that you understand your policy. What is covered, what are the expectations and responsibilities, and what are the covered events?

#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...

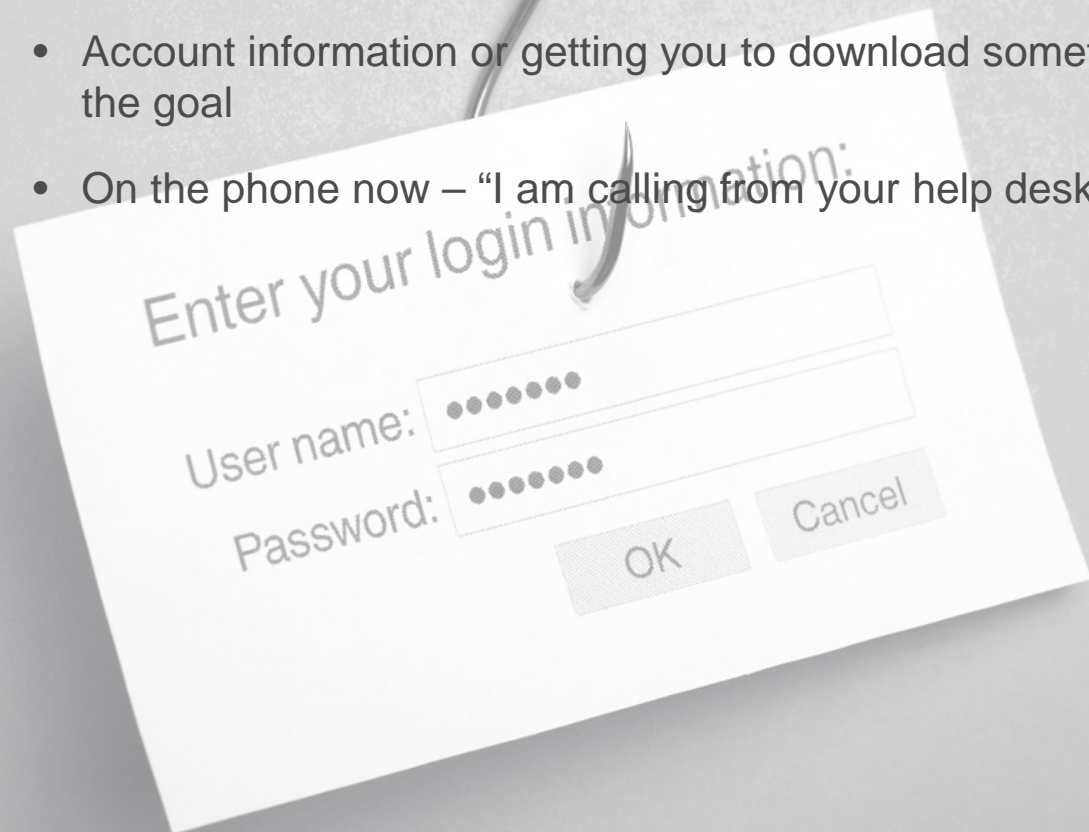
1. Does not cover your reputation
2. Expensive for good coverage
3. Effective if you have the right coverage
4. The biggest loss to an organization is the loss of business and customer trust

#8

ADVANCED PHISHING SCAMS

THE RISKS ARE ALL RELATED

- The world of fakes – deception through realistic appearing texts, emails
- A bit easier since a lot of organizations use third-parties to “update your claim account information”
- Whaling
- Account information or getting you to download something is the goal
- On the phone now – “I am calling from your help desk”



#8

ADVANCED PHISHING SCAMS

THEY'VE GOTTEN BETTER

From: VISA
Subject: Billing Information
To: Steve Pain
Cc:

VISA — USE OF A TRUSTED COMPANY LOGO

Dear Visa customer, **GENERIC SALUTATION**

This email is to inform you of a recent update we made to our systems, **UNPROFESSIONAL MANNER**
To avoid service interruption we require that you confirm your account as soon as possible.

Please take a moment to confirm your account by going to the following address:


http://visa-secure.com/personal/secure_with_visa/ **POSSIBLE DISGUISE FOR WWW.VISA.COM**

Follow these steps:

- 1: Confirm your account by clicking the link above.
- 2: Verify your visa card information.
- 3: Your account will then be updated, you may continue using your visa without any in **STATEMENT URGING IMMEDIATE ACTION**

***** Please note: If you FAIL to update your visa card, it will be temporarily disabled.**

We apologize for any inconvenience this may cause.
The visa team is working hard to bring you the best



Dear iTunes Customer!

Your iTunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

[Get Started](#)

If you need <http://goo.gl/Gkx2HM> Help left by clicking the Help link located in the upper right-hand corner of any Apple page.

Sincerely,
Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

#8

ADVANCED PHISHING SCAMS

WHAT CAN YOU DO?

Always be a skeptic.

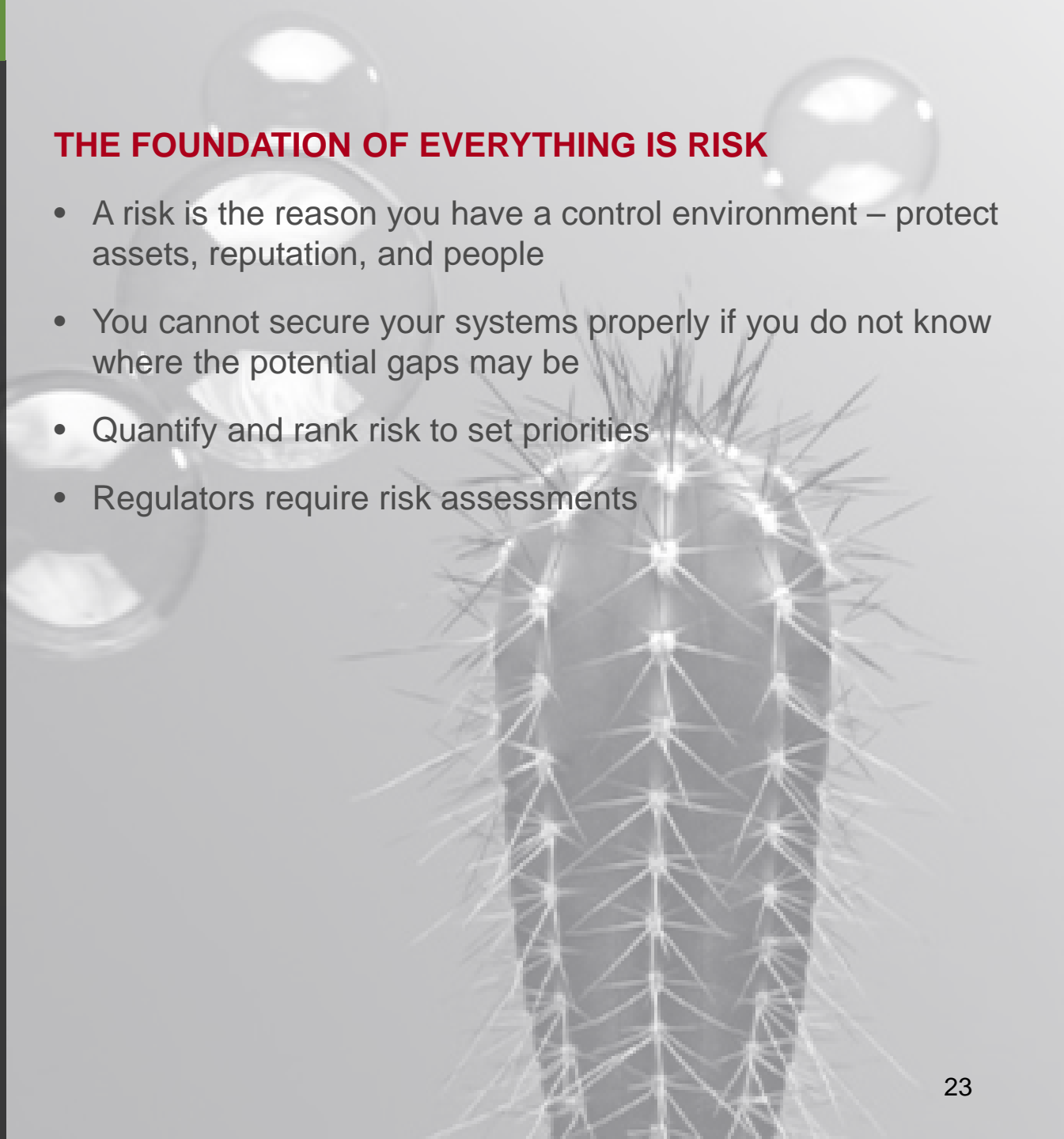
- If it looks fake, it is fake. Call the company from the number on your card or statement.
- Companies do not email customers over account information
- Hover over the link....
- Security awareness training
- Social engineering testing
- Email filters, antivirus, patching



#9

LACK OF IT SECURITY RISK ASSESSMENTS

THE FOUNDATION OF EVERYTHING IS RISK

- A risk is the reason you have a control environment – protect assets, reputation, and people
 - You cannot secure your systems properly if you do not know where the potential gaps may be
 - Quantify and rank risk to set priorities
 - Regulators require risk assessments
- 




#9

LACK OF IT SECURITY RISK ASSESSMENTS

WHAT CAN YOU DO?

- Risk Management Program
- Pick a framework – CoBit, COSO, NIST, etc.
- Re-visit annually
- This is not an easy nor quick project

RISK RANKING

RISK	LIKELIHOOD TO OCCUR	IMPACT OF RISK			OVERALL RISK RATING
		Financial	Security	Operational	
 Low	Low likelihood: 1	Low impact: 1	Low impact: 1	Low impact: 1	Low overall risk: 4 - 5
 Medium	Medium likelihood: 2	Medium Impact: 2	Medium Impact: 2	Medium Impact: 2	Medium overall risk: 6 - 8
 High	High Likelihood: 3	High Impact: 3	High Impact: 3	High Impact: 3	High overall risk: 9 - 12



#10

ADVANCED RANSOMWARE

RANSOMWARE IS IMPACTFUL

- System lockout through encryption
- Entire network encryption and lockout (worm)
- Webpage Denial of Service Attacks

IMPACTS:

1. Humiliation of victims – Ashley Madison
2. Reputation loss – we locked out Target!
3. Loss of business – What if Amazon.com went down for 10 minutes?

#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
- Antivirus software
- Software whitelisting
- Incident response plan
- Micro-segmentation
- Email filtering for executable files

Contact Us

TINA BODE

Manager
tbode@berrydunn.com
207.541.2253

Reviewed:
09/29/17

