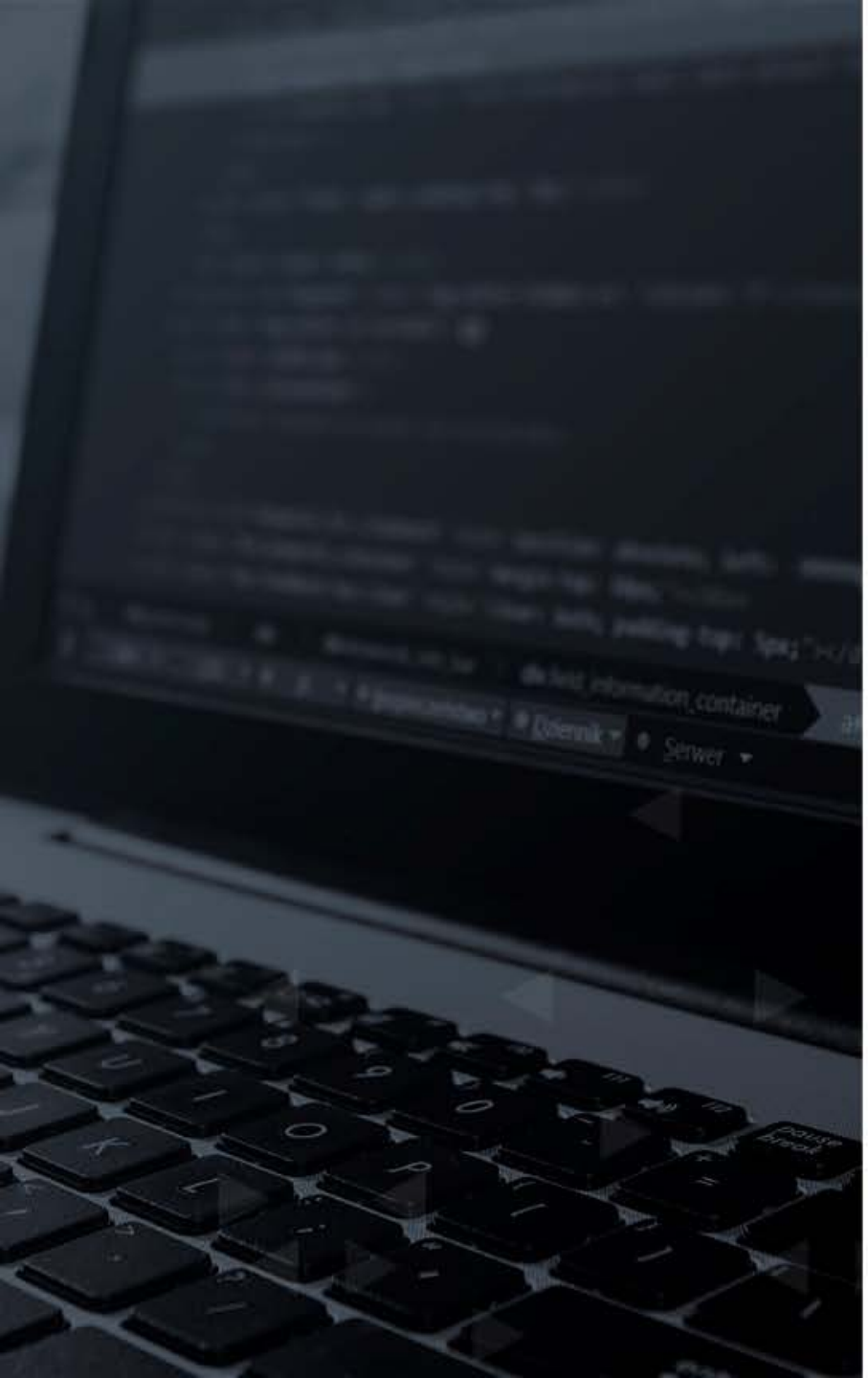
Everyone needs a trusted advisor. Who's yours?



Audit-Compliance-Risk:

Internal Responsibility in Cybersecurity

Philip Diekhoff, CISSP, CISA

Managing Consultant, BKD Cyber

BKD CYBER

The State of IT Security

"IT USED TO BE THAT IF YOU WORRIED ABOUT UNSEEN FORCES YOU WERE CONSIDERED PARANOID. NOW YOU'RE A SECURITY EXPERT."

BKDCYBER

Objectives

- Definitions
- Discuss the ever-evolving landscape of cyber threats & risks
- Talk about the top ten BKDCyber cybersecurity areas – discuss how credit unions & credit union members can work together for the common good
- Identify steps individuals & credit unions can take to help minimize effects of cyber threats through employee accountability, responsibility & governance

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Definitions

Cybersecurity

- The process of protecting information by identifying, defending against, responding to & recovering from attacks[1]

1 - NIST

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Definitions

Cybersecurity

- In recent security discussions, there are references to both “cybersecurity” & “information security.” The terms are often used interchangeably, but in reality, cybersecurity is a part of information security

Everyone needs a trusted advisor. Who’s yours?

BKDCYBER

Cost of a Data Breach

- Average total cost of a data breach - **$3.92 million**
- Average total cost in the US - **$8.19 million**
- Average size of breach – **25,575 records**
- Average per record - **$153 worldwide, $320 in US**
- Time to identify and contain breach – **279 days**

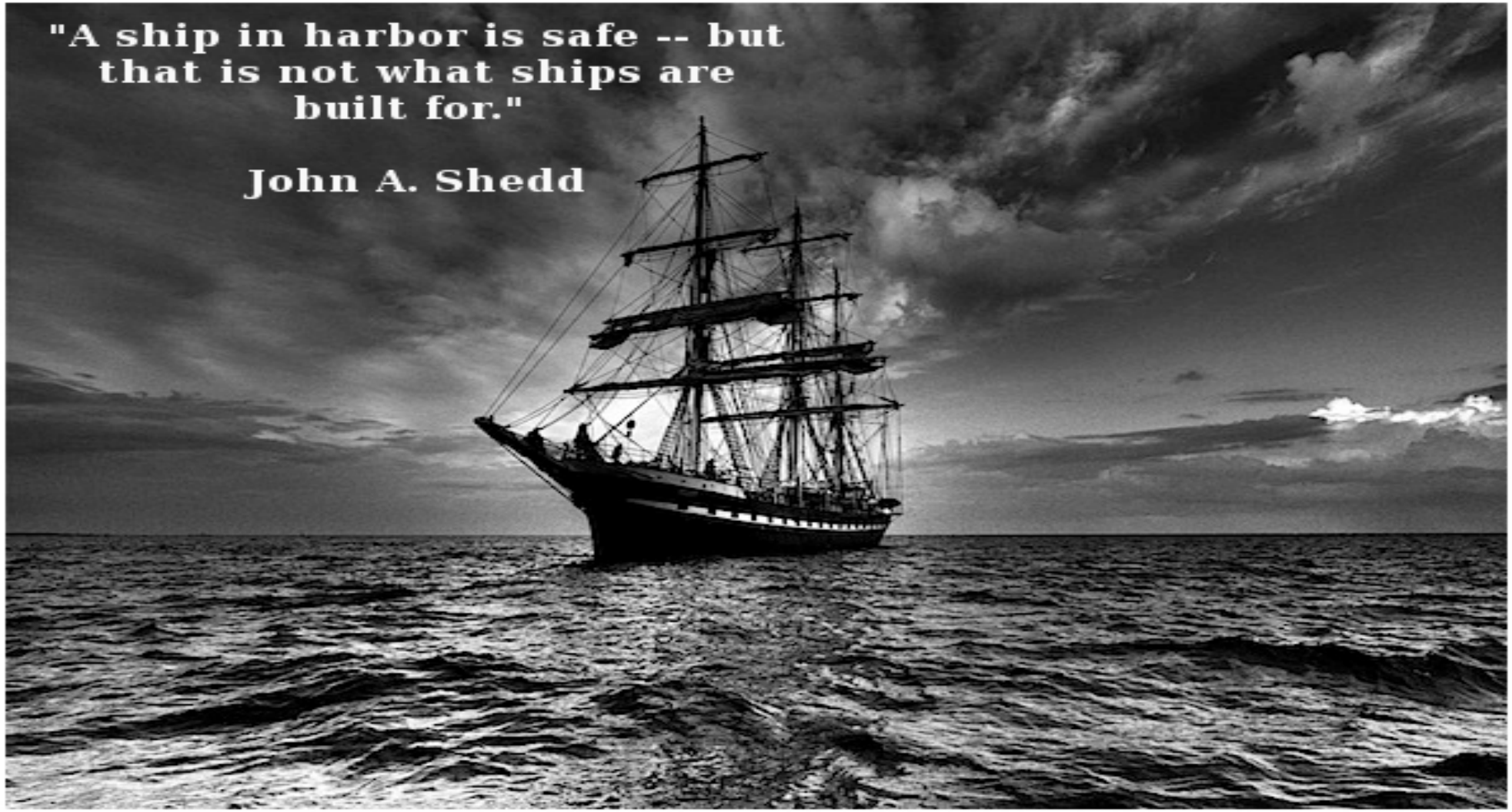
1 – Cost of a Data Breach 2019, IBM Security

Cost of a Data Breach

- Some Breach Facts
  - Cost includes lost of business
  - Cost goes on for years
  - Malicious attacks are the most expensive
  - Encryption, BCP and Threat Intelligence sharing (FS-ISAC) mitigate cost
  - Companies with Incident Response team mitigated cost

1 – Cost of a Data Breach 2019, IBM Security

BKDCYBER's
Top 10 – Opportunity for Governance



BKDCYBER

#1 – Know Where Your Data Is Stored

Document & maintain accurate information asset inventories, including all relevant assets that store or transmit sensitive data *(devices & software – use software like Track-It)*

- Conduct, document & maintain current data flow analysis to understand location of your data, data interchange & interfaces, as well as applications, operating systems, databases & supporting technologies that support & impact your data *(Use white board to create flow charts to document processes, etc.)*
- Locate & consolidate all valuable data into most singular storage possible; by reducing footprint of your data you create fewer potential vulnerabilities, as well as minimizing effort of monitoring & tracking access to that data

BKDCYBER

#2 – Know Who Can Access Your Data

Align logical & physical access authorization, establishment, modification & termination procedures applicable to networks, operating systems, applications & databases

- Screen employees prior to employment
- Document additions & modifications with standard change management
- Timely removal of terminated employees
- Limit Vendor Remote Access
- **Administrator Access**
- **Segregation of Duties**

BKDCYBER

#3 – Perform Risk Assessments

Perform an information security risk assessment that is flexible & responds to changes in your environment. Specific focus should be on all protected information & protected GLBA information (if applicable)

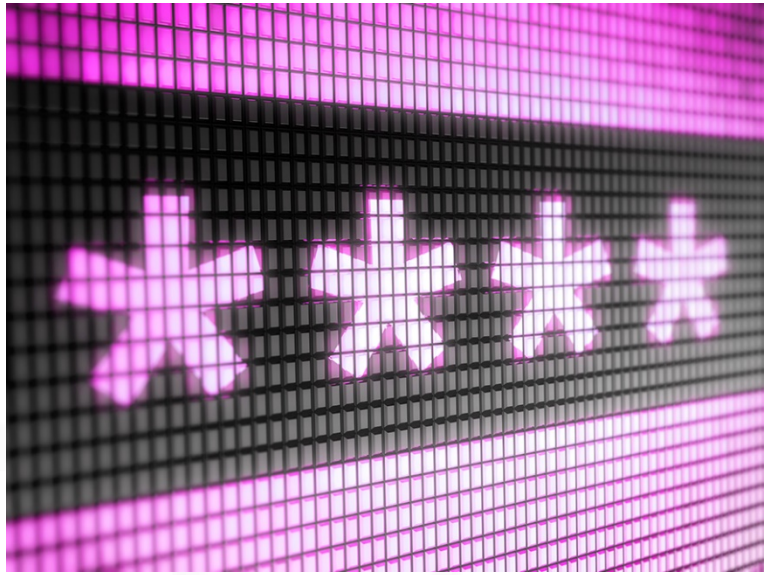
- Asset-based format
- Identify foreseeable threats
- Determine likelihood of occurrence
- Determine magnitude of impact
- Assign inherent risk rating
- Input mitigating controls
- Determine residual risk rating
- Update annually to adjust for new threats

BKDCYBER

#4 – Take Advantage of Security Controls

Establish, implement & actively manage security configuration settings for all hardware & software for servers, workstations, laptops, mobile devices, firewalls, routers, etc.

- System/device hardening
- **Strong password security**
- Limit administrative privileges
- Grant only the minimum required access to perform job functions



BKD CYBER

Athena

Dedicated Password Cracker

We utilize Hashcat, power of the Nvidia video cards

We increased speed from previous device by close to 100 times

We have cracked passwords up to 16 characters, complex

Dictionary words easiest to crack

BKDCYBER

Accountability – Avoid These Common Password Pitfalls

Current month or season	A holiday	City or street where you are located
Child's name with a number (especially a birth year)	Name of a popular song/nursery rhyme/religious passage	"Password" or "I hate passwords"
Vulgarity or racial slurs	Name of Windows service	Name of common network protocols

CRACKED PASSWORDS

$central1
$$Zack$$
tommyh14!
pay$1596
Twins123%
qwert123Q!
gnik.Tk75
tyui-789
zxcv-5987

Cracking 28% of bank & CU passwords recently!

BKD CYBER

#5 – Implement Data Loss Prevention Controls

Organizations must limit access to removable media, CD ROMs, email & file transfer websites

- Leverage group policies & existing software such as content filtering, email filters, etc., **Layered Security**
- Companies should write clear, well-planned policy that encompasses device use & disposal of information
- When devices are no longer in use, data should be wiped & then physically destroyed

BKD CYBER

#6 – Ensure All Critical Data Is Encrypted

Adoption of data encryption, for data in use, in transit & at rest, provides mitigation against data compromise

- Encrypt all hard drives on all portable devices, conducted in conjunction with #1
- Data backup, retention & archival information should all be under protection of strong encryption to ensure such data that may fall into malicious hands cannot be interpreted &/or otherwise utilized

Note – In event you lose device, compliance mandates may require you to <u>prove</u> the device was encrypted.

BKDCYBER

#7 – Effective Patch Management

Ensure all systems, regardless of function or impact, have recent operating systems, application patches applied & any business-critical applications are maintained at the most current feasible level for your organization

- Evaluate & test critical patches in timely manner
- Apply patches for riskiest vulnerabilities first
- Use WSUS (or other tool) to manage Windows-related patches
- Third-Party Applications (Java, Adobe, Flash, etc.) must also be managed

Be strategic & plan for end of life events (for example, Windows 7 & Server 2008 expire **January 2020**)

BKDCYBER

#8 – Educate Personnel & Hold Them Accountable

Provide staff training on security best practices, internal policies & new threats. Focus on social engineering, phishing & physical security concerns

- Educate all personnel, at least annually, on your company's data security requirements
- Education can be as simple as email reminders, brown bag lunch & learns, etc.
- Make sure new-hire onboarding process includes this topic
- Accountability includes ALL personnel—especially senior management—who must lead by example

BKD CYBER

Social Engineering

- Starts with profiling the organization
  - Obtain IT director’s name
  - Prepare strategy for exploit
  - Mock up website
  - Originate email campaign
  - Harvest user names & passwords
  - Execute exploitation strategy
  - Experience 5% to 46% of users tested provide info
    - Getting better in last 6 months (1–2% to 7–8%)

BKDCYBER

#9 – Audit & Assess Controls

Conduct vulnerability scans & penetration tests to identify & evaluate security vulnerabilities in your environment

- Security controls provide most value when they are audited & monitored for compliance &/or maintenance
- Annual audits provide necessary insights into keeping security controls optimized & properly fitted to environments employed to protect

BKD CYBER

#10 – Minimize Impact by Taking Immediate Action

Management's ultimate goal should be to minimize damage to the institution & its members through containment of the incident & proper restoration of information systems

- Conduct analysis of past incidents & applicable responses to determine successful & unsuccessful areas
- Use an incident response team to ensure immediate action is taken following security event to minimize impact on operations & loss of data
- Determine who will be responsible for declaring an incident & restoring affected computer systems once the incident is resolved

Frameworks

- FFIEC IT Handbooks
  - 11 handbooks (Audit, BCP, IS, etc.)
- GLBA
- Cybersecurity Assessment Tool (CAT)
  - Automated Cybersecurity Examination Tool (ACET)
  - FSSCC Cyber Profile
- InTREx

BKDCYBER

IT Audit Functional Areas

- Management / Governance
- Information Security / Cybersecurity
- Physical Security
- Network Logical Security
- User Administration
- Change Management
- Business Continuity / Disaster Recovery
- Electronic Banking
- Vendor Management

BKDCYBER

IT Audit Preparation - Governance

- Complete the **FFIEC Cybersecurity Assessment** annually and **address gaps promptly**
- Ensure information security, BIA, BCP/DR, & incident response **policies** & **procedures** address Cybersecurity
- Ensure adequate **IT strategic plans** & **budgetary resources** are provided to the Board
- Incorporate Cybersecurity into the **risk-based audit plan**
- Ensure **enterprise wide** awareness training is performed (educate & motivate)
- Ensure the **Information Security Officer** has adequate authority, resources & independence **(Management Booklet November 2015)**
- Include **cyber events** in annual disaster recovery tests
- Join **Financial Services – Information Sharing & Analysis Center (FS-ISAC)** or other information sharing forums – filter reports based on each employees' role
- Ensure **threat intelligence** is timely, ongoing, risk focused, reported & actionable

BKD CYBER

IT Audit Preparation - Technical

- Track, report, independently test & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Rename **network admin** accounts, **separate** production & admin login privileges & **do not share** network admin login credentials
- Maintain accurate **asset inventories** & be aware of **ports of entry** (you can't protect what you don't know exists)
- Enforce **application whitelisting** controls
- Implement **data loss prevention controls** (USB ports, email, etc.)
- Use **encryption** to protect confidential data
- Do not use **weak** or **default** passwords
- **Limit** local administrator rights
- Update **anomaly detection** tools regularly & understand configurations
- Use **log analyzers** (Security Information & Event Management – SIEM tools) to wade through the false positives & assign responsibility for log review

BKDCYBER

Top 5 Gaps

- Unauthorized Devices / Software / Users
  - FFIEC Information Security Work Program, Objective II: M-9
- Testing Patches
  - FFIEC Operations Booklet, page 22
- Firewall Rules – Quarterly
  - FFIEC Information Security Booklet, page 82
- Removable Media
  - FFIEC Information Security Work Program, Objective I: 4-1
- Anomalous Activities
  - FFIEC Information Security Booklet, page 32

BKDCYBER

Other Notable Gaps

- **IS Policies** are not commensurate with organizational risk and complexity that address the concepts of threat information sharing.
- A normal **network activity baseline** is not established. (FFIEC Information Security Booklet, page 77)
- **Data flow diagrams** are not in place and document information flow to external parties. (FFIEC Information Security Booklet, page 10)
- **Customer awareness** materials are not readily available. (FFIEC E-Banking Work Program, Objective 6-3)
- **Elevated privileges** are not monitored. (FFIEC Information Security Booklet, page 19)

BKDCYBER

Who Came Up with This?

Questions?

Thank You!

BKDCYBER

BKD Thoughtware®

- Webinars, seminars & articles
- Many are CPE-eligible
- PDMs – Populate bullets with most relevant webinars, articles, videos, etc.