



perspective
GAINED

OCTOBER 12, 2018

CYBERSECURITY RISK: KEEPING YOUR BOARD INFORMED

Chris Ellingwood, Senior Manager | Lindsay Spain, Senior Consultant





1 WHY BOARDS SHOULD CARE ABOUT CYBERSECURITY

2 EXTERNAL GUIDANCE

3 RESPONSIBILITIES:
Management vs. Board

4 RECOMMENDATIONS

CONSIDER THIS ...

**\$6
TRILLION**

Amount criminals will bring in annually from cybercrimes by 2021
(More than the illegal drug trade market)

3rd

Rank of the financial services industry as a targeted business type
(Healthcare is number 1)

14%

Percentage of Boards and Directors that say they are actively involved in cybersecurity at their company

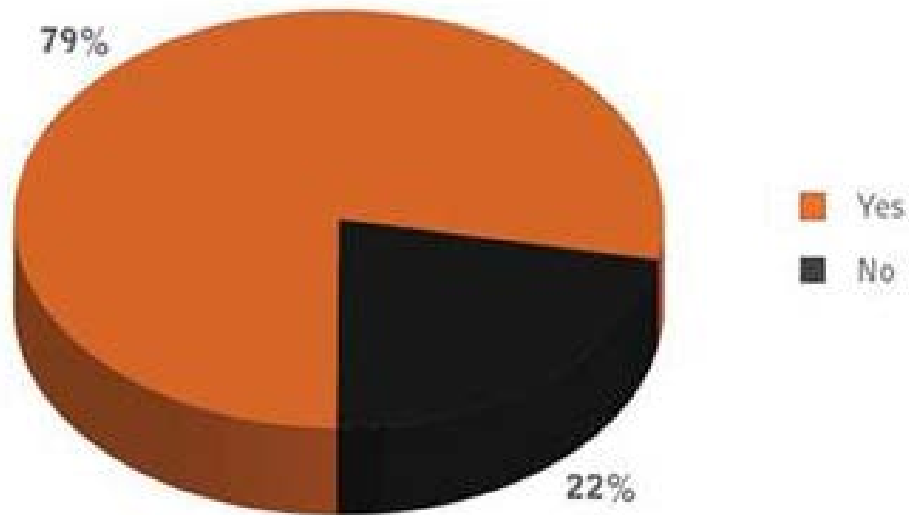
**FDIC
FINDINGS**

Common IT findings include:

- An “under-utilized risk management program”
- Lack of reporting to the Board

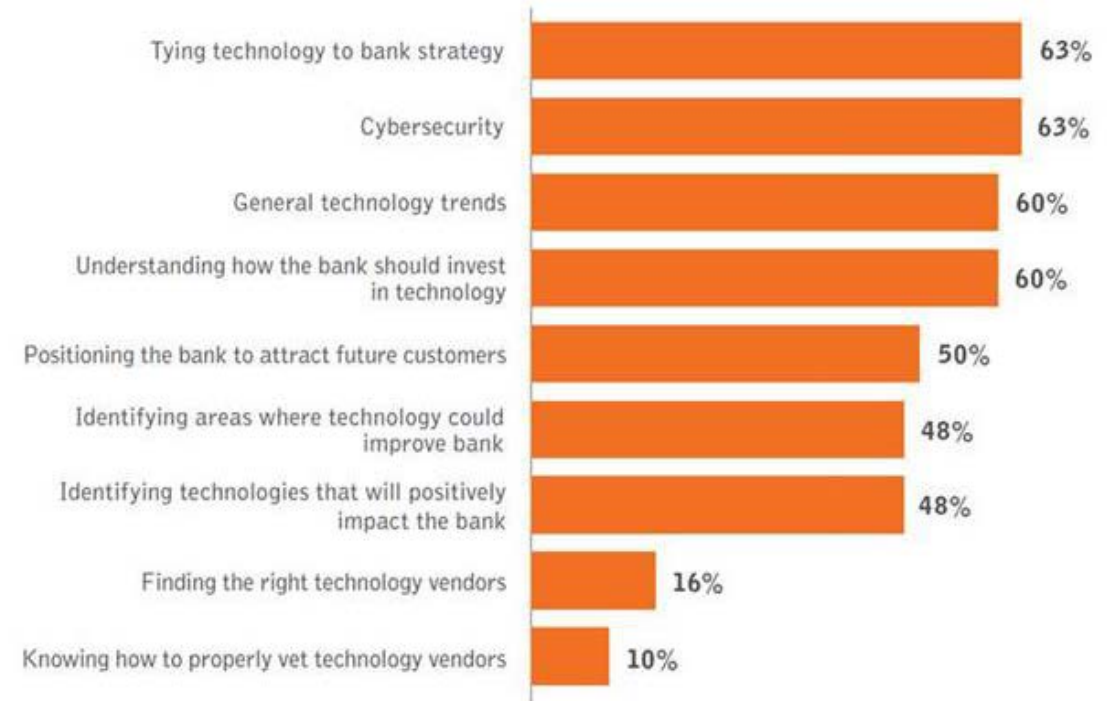
CONSIDER THIS ...

In your opinion, does the board as a whole need to enhance its level of expertise regarding technology?



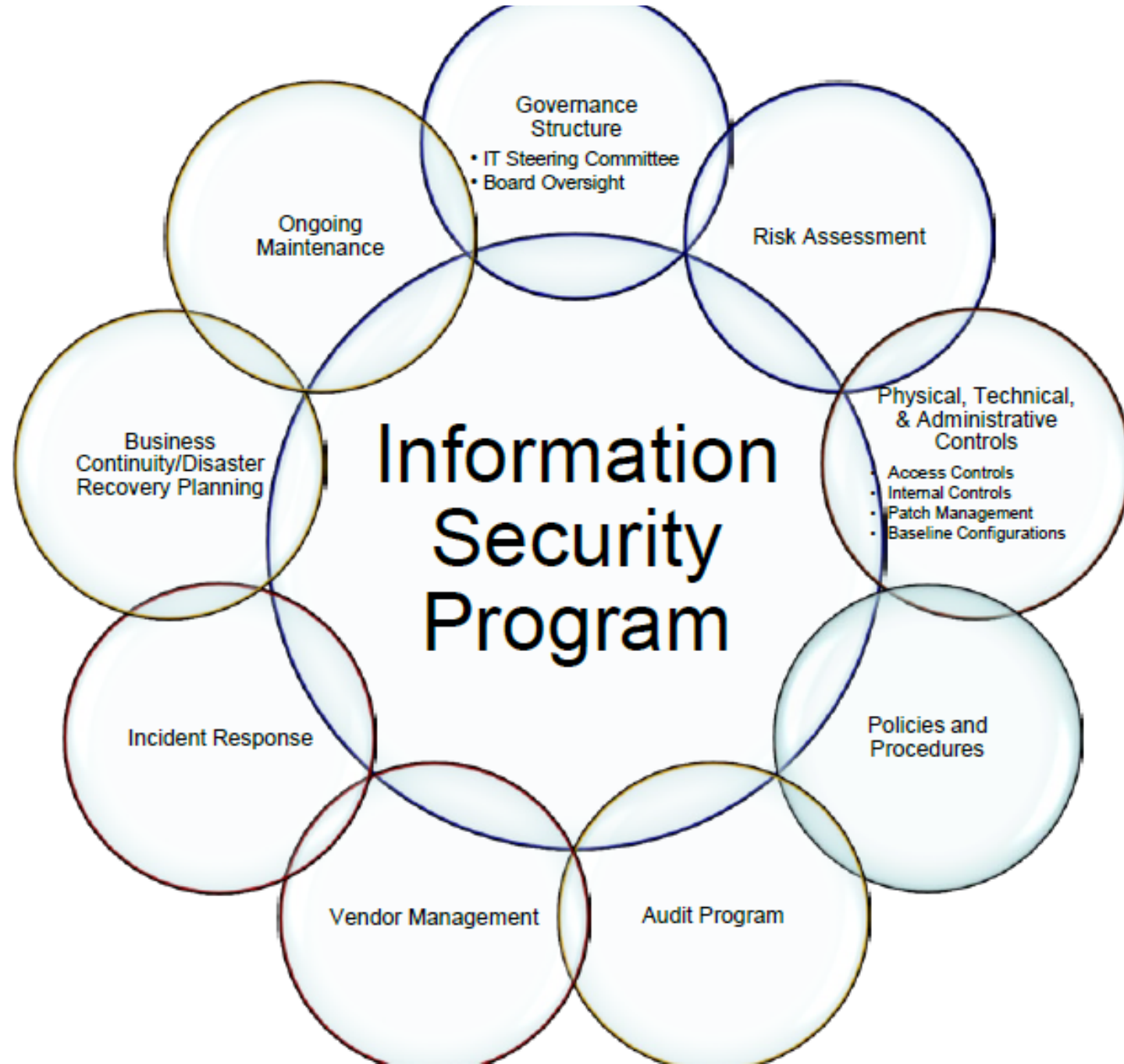
Where does the board need to improve its knowledge of technology?

Respondents were asked to select all that apply.



FDIC

APPROACH TO INFORMATION SECURITY



FINANCIAL IMPACT OF A DATA BREACH

REMEDIATION COSTS

(Cost to fix the actual infrastructure and systems, replacement debit/credit cards)

1

LOST REVENUE AND REPUTATIONAL IMPACT

(Customer mistrust, system downtime, etc.)

2

LITIGATION COSTS

(Mailings and notifications, court fees, attorneys, and sanctions or fines)

3

INCREASED INSURANCE PREMIUMS

(Cyber insurance and liability insurance)

4

BOARD RESPONSIBILITIES

DISCLOSURES (SEC REPORTING)

- Materiality when assessing cybersecurity incidents
- Cybersecurity Risk Management Program
- Oversight role of the Board
- Board's engagement with management

CONTROLS AND PROCEDURES

Assess impact to determine whether to disclose

PROPOSED LEGISLATION

In 2017/2018 the SEC proposed a new requirement that the Board of a public company must have someone who is knowledgeable of cybersecurity on the Board. If not – the board must explain why they are still aware of IT Security and Risk, and how.



ENTERPRISE RISK MANAGEMENT

INTEGRATING WITH STRATEGY AND PERFORMANCE

- Risk management is not an isolated exercise
- Linked to overall performance
- Connect with stakeholder expectations
- Proactive not reactive

5 PRINCIPLES OF THE BOARD

1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4

Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

5

Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.



SYSTEM AND ORGANIZATION CONTROLS REPORTING

- Enterprise risk management – this is a company-wide effort
- **Vendor** risk management – You are still responsible
- Disclosing incidents
 - Cybersecurity
 - Loss of confidential data
 - Breaches in service commitments

UNDERSTAND

- Risks
- Impact
- Investments
- Oversight vs. management

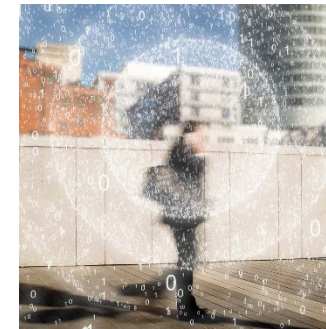
1



COMMUNICATE

- Review strategy, policies
- Review incident response and disaster plans
- Establish metrics

2



TAKE ACTION

- Get educated on the risks
- Assess Board committees and skills
- Assess cyber insurance
- Perform crisis simulations

3



UNDERSTANDING RISKS & IMPACT

- What are the IT Security risks to my company?
- How are risks mitigated?
- Have risks been cataloged?
- Are they updated at least annually?
- Are they updated after changes?
- What are emerging risks we should be aware of?



DISCUSSION:

- What is the biggest IT security risk to your organization?
- What are you doing to address it?
- Is the board aware?



COMMUNICATE CYBERSECURITY METRICS

- Establish reporting to the Board
- Incidents, hacking attempts, breaches
- Vendors and the risks associated with them

ACTION




DO YOU HAVE CYBERSECURITY INSURANCE?


Discuss the needs with the Board

WHAT DOES IT COVER?

- Remediation costs?
- Fines?
- Litigation?

ONGOING MONITORING RISK REGISTER

Risk:	Likelihood to occur	Impact of risk			Overall risk rating
		Financial	Security	Operational	
 Low Risk	Low likelihood: 1	Low impact: 1	Low impact: 1	Low impact: 1	Low overall risk: 1 - 9
 Medium Risk	Medium likelihood: 2	Medium impact: 2	Medium impact: 2	Medium impact: 2	Medium overall risk: 10 - 19
 High Risk	High likelihood: 3	High impact: 3	High impact: 3	High impact: 3	High overall risk: 20 - 27

Category	Number of Risks
 Low Risk	2
 Medium Risk	2
 High Risk	0

Risk Profile A – Personnel Security

Overall Risk



Risk Profile B – Security of Financial Transactions

Overall Risk



Risk Profile C – Security of Vendors and Vendor Due Diligence

Overall Risk




Risk Profile D – Computer, Data Communications, Database, and System Security

Overall Risk



ONGOING MONITORING

- Cybersecurity risks included in risk register
- Updated for changes throughout the year
- Included in Board agenda at least annually



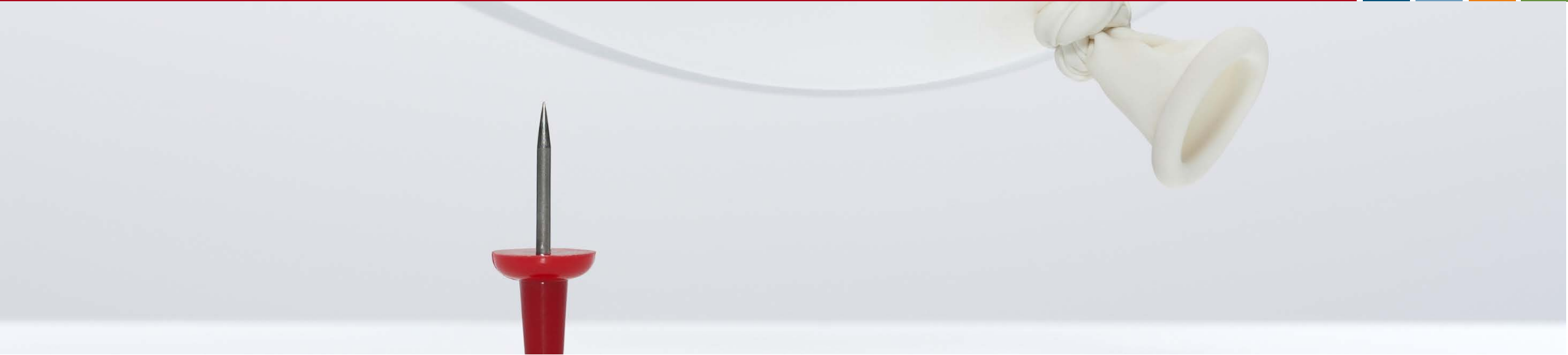
- Does the Board know how to measure the effectiveness of your cybersecurity program?
- Does the Board ask for follow up on progress?
- Does the Board ask for follow up on any IT-related audit findings?



ONGOING MONITORING

REPORT MONTHLY METRICS TO THE BOARD

- Incidents and cause and resolution
- Suspicious activity
- Emerging threats



ASSESS BOARD SKILL SETS

The Board needs sufficient members who understand cybersecurity risks

CYBERSECURITY INSURANCE

Determine your risk appetite with the Board – this is the last resort



SEEK THIRD PARTY HELP

- Offer to train and educate the Board on risks
- Do they undergo the same security training as your employees?

ASK QUESTIONS

- Encourage the Board to ask questions of you and your auditors
- Ensure they understand the potential impact of an exposed risk



BOARDS AND SENIOR MANAGEMENT ARE TARGETS

- Fake emails that attempt to collect data, credentials, or a financial gain
- Board members and Sr. Management are often exempt from policies
- Access to high level of information
- Ability to influence others
- “Non-employees” who use personal devices



QUESTIONS



CHRIS ELLINGWOOD

SENIOR MANAGER

cellingwood@berrydunn.com



LINDSAY SPAIN

SENIOR CONSULTANT

lspain@berrydunn.com