



Grant Thornton

An instinct for growth™

The CFO's Role in CyberSecurity...



Johnny Lee

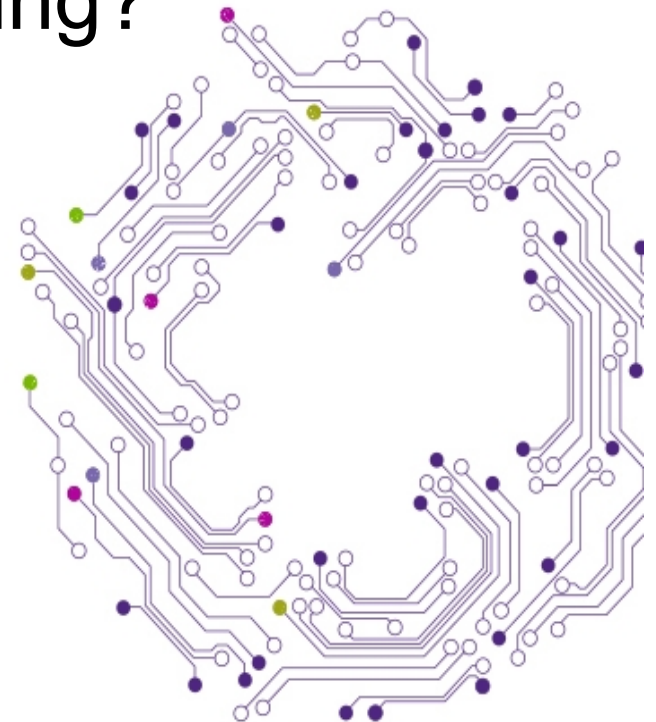
Managing Director

Forensic, Investigative & Dispute Services

Grant Thornton LLP

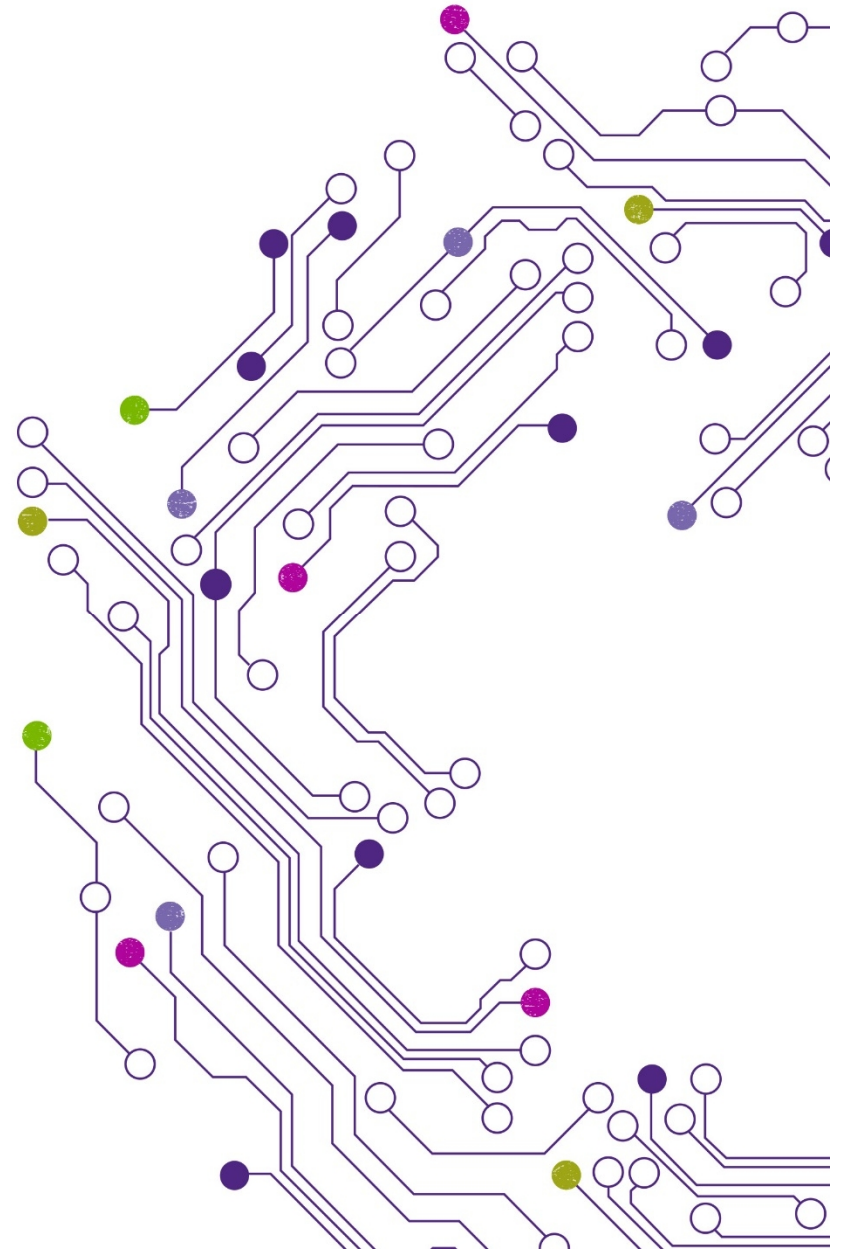
Agenda

- Key research findings and analysis
- What should companies be doing?
- What should CFOs be doing?
- Questions



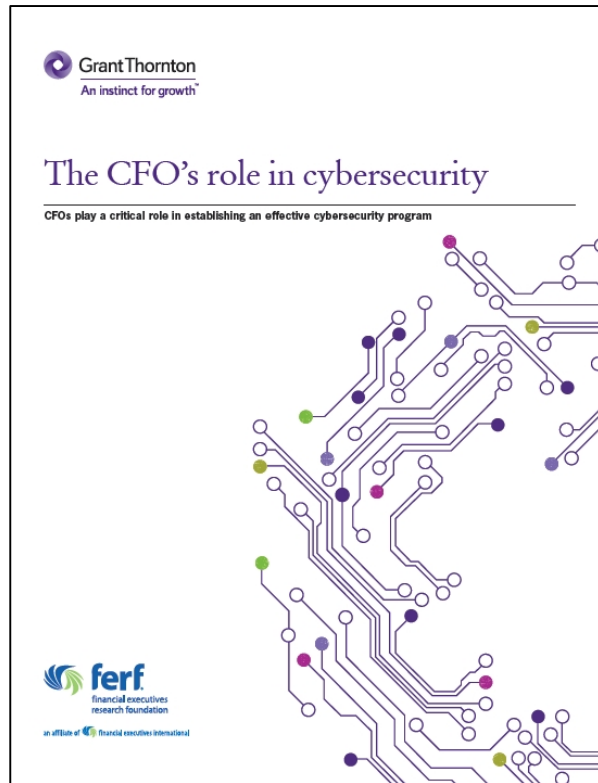
AGENDA

Key research findings and analysis



The CFO's role in cybersecurity

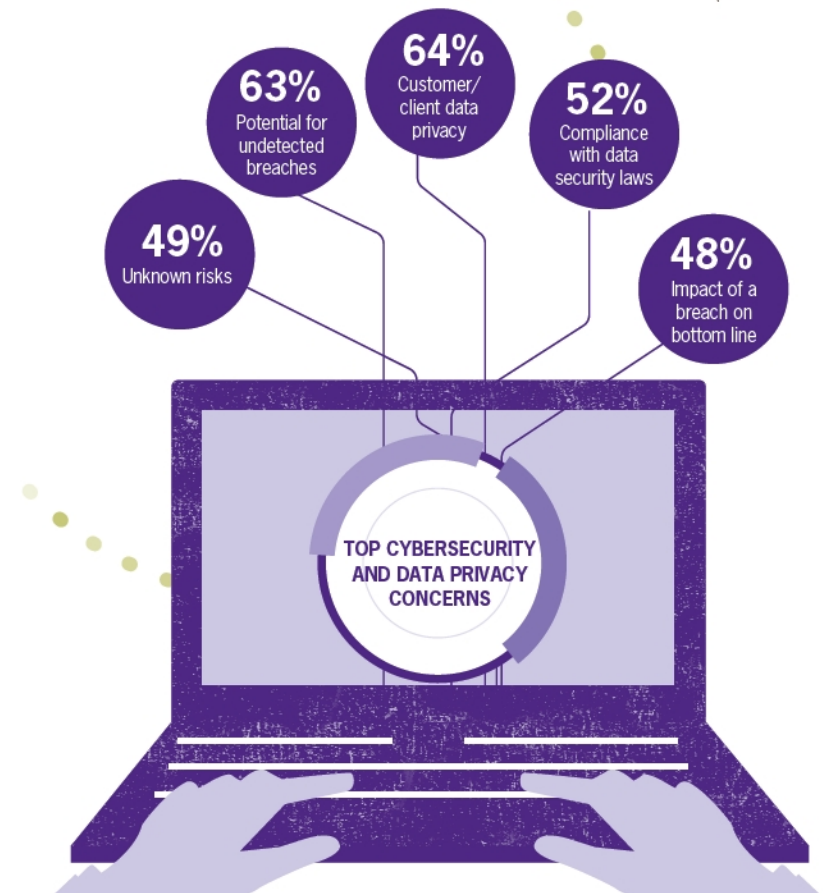
Research collaboration with Financial Executives Research Foundation



- CFOs play a critical role in keeping organizations secure from cyber threats. From establishing an effective cybersecurity program to interfacing with the board, their responsibilities are crucial to the success of the business.

Data privacy and potential for breaches are top concerns

- Many CFOs are unaware of items they should be protecting
 - Data that leaves the four walls of their organization when it is shared with a third party or vendor
- Cybersecurity concerns vary considerably depending on the particular business

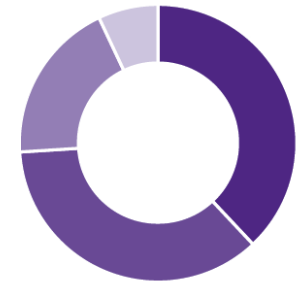


The responsibility for cybersecurity should be shared

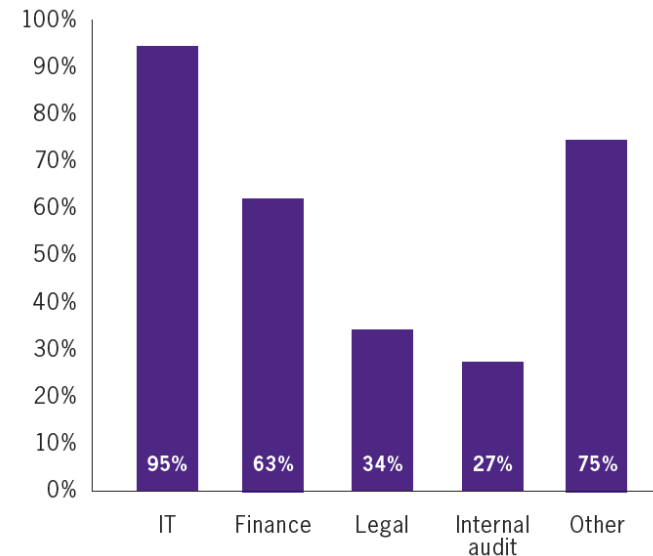
- 76% of respondents indicate that more than one department is involved
- Only 34% of respondents say the legal department is involved in cybersecurity efforts
- While cybersecurity was once relegated to a technical or operational issue handled by IT, a cross-departmental, enterprise-wide approach to cybersecurity is necessary, according to the NACD's *Cyber-Risk Oversight, Directors Handbook Series*

Who is responsible for cybersecurity?

- CFO **38%**
- CIO **36%**
- Other **19%**
- CISO **7%**



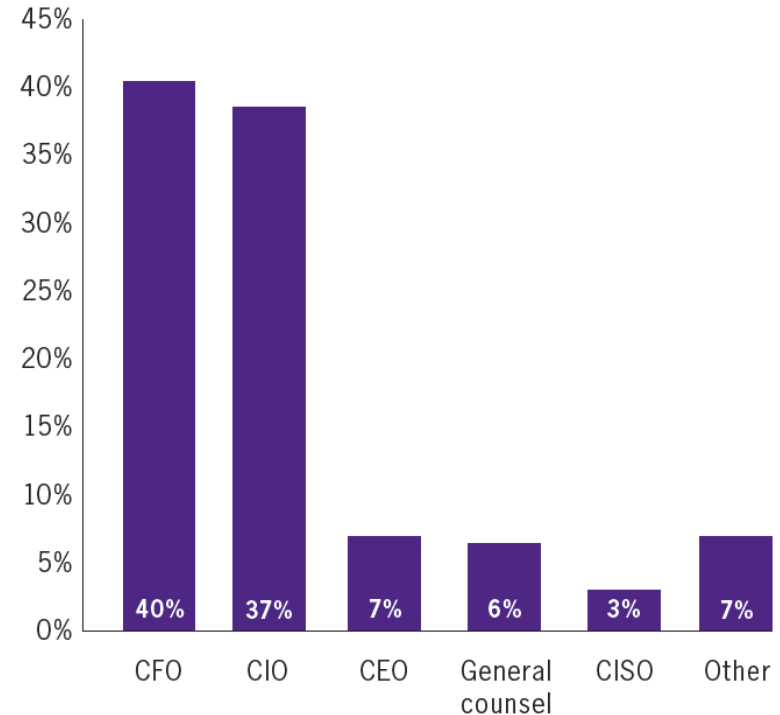
Which departments are involved with cybersecurity efforts?



CFOs should initiate the cyber discussion

- Not only should the CFO (or CIO) be reporting to the board on the organization's cybersecurity initiatives, but he/she should also be getting buy-in from the board on necessary cyberinvestments and advocating for cybersecurity resources
- As the potential loss for each attack could range in the millions, it is imperative that boards focus closely on cybersecurity oversight, and the CFOs introduce the discussion

Who is responsible for reporting to the board about cybersecurity?



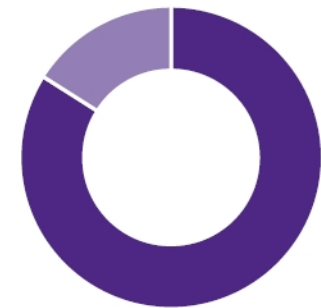
A cybersecurity task force is critical, and should include IT, legal, and finance

“ Companies that have task forces, as well as those that have experienced breaches, have a much greater awareness of cybersecurity risks, and tend to have a more robust role for their legal function. ”

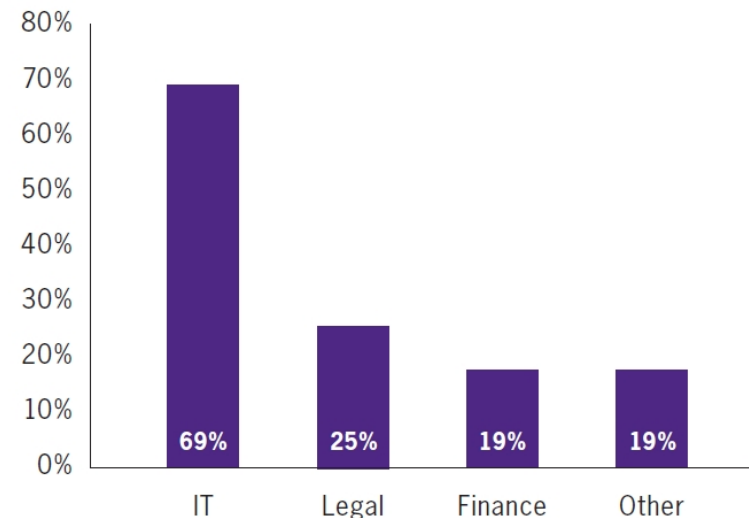
-Partner at global law firm

Does your organization have a cybersecurity task force?

- No **84%**
- Yes **16%**



If yes, which areas of business are on the task force?



Organizations may not be doing enough to safeguard against cyber threats

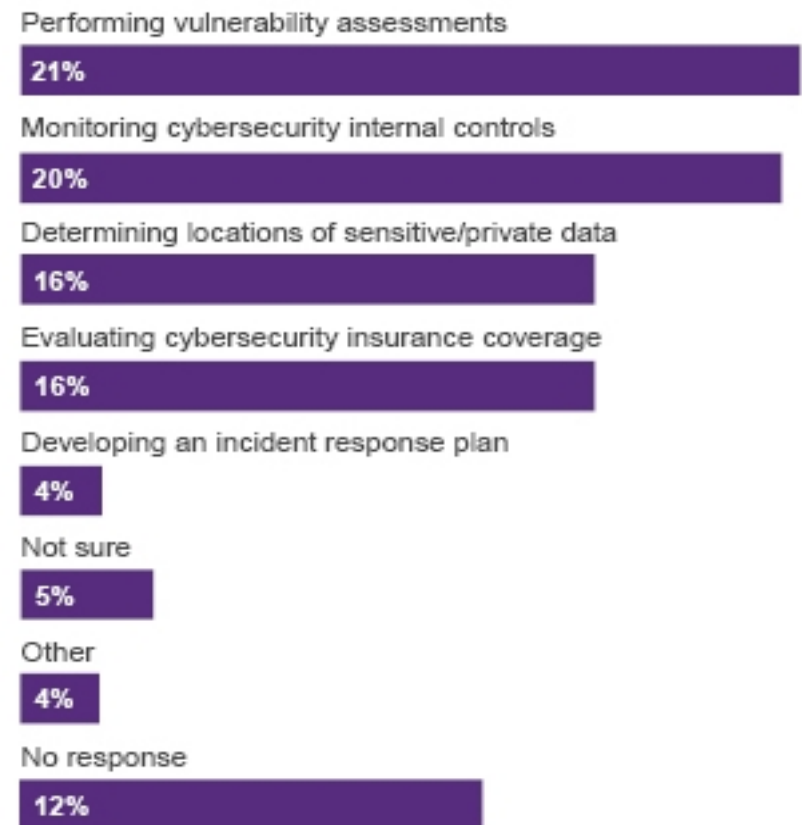
"Even if an organization has not been subject to an attack, it does not mean that efforts to secure information systems should be tabled...Any company with data systems connected to the Internet is at risk of a breach."

Has your organization experienced a cybersecurity breach?

- No 74%
- Yes 14%
- Not Sure 11%



What steps is your organization taking to respond to cybersecurity risks?



Common Misconceptions...

It will never happen to me

Our network is secure

We are not a big company



We don't have any personal information, so we aren't a target

We have never been attacked

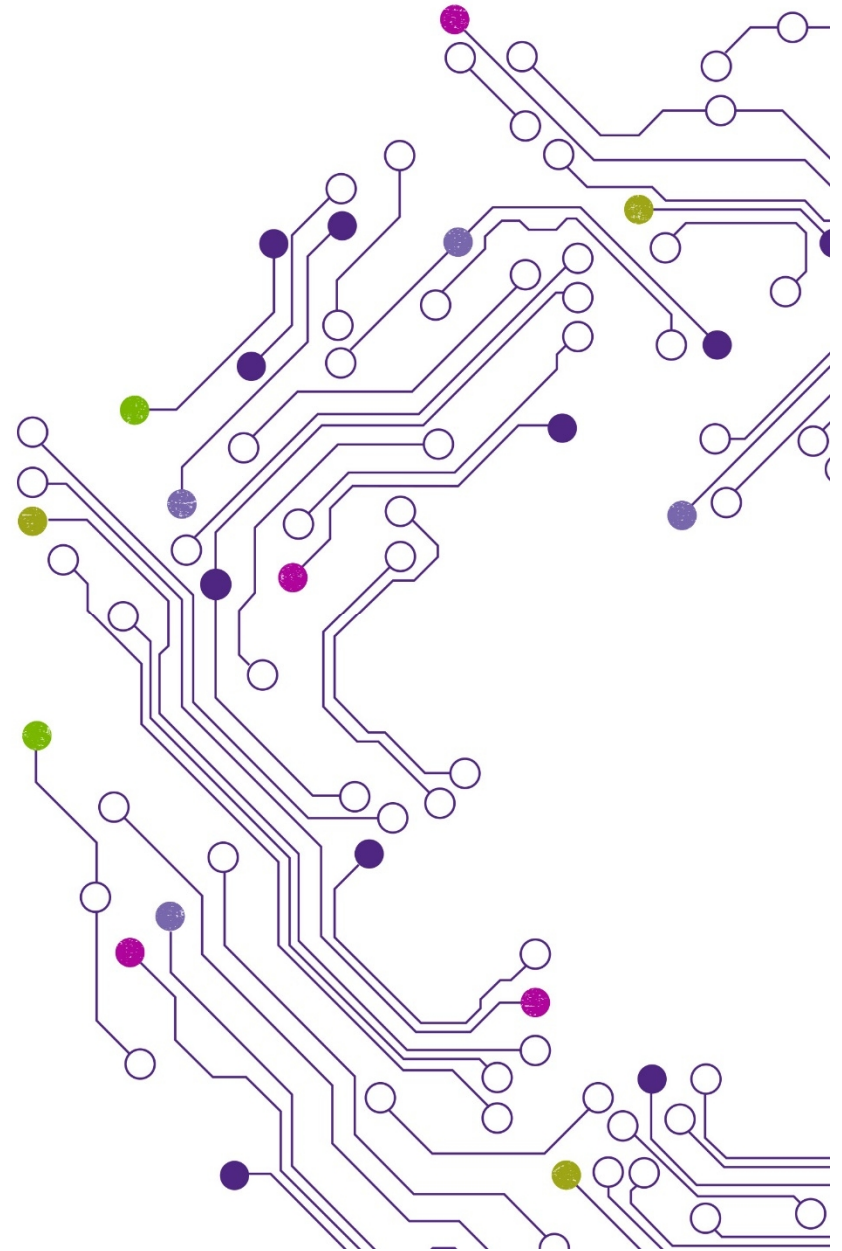
Major impediments to developing an enterprise-wide cybersecurity strategy

- The most common impediment to developing an enterprise-wide cybersecurity strategy is a **lack of understanding of the risks and potential impacts of a breach**
- This common issue **leaves valuable information exposed**



AGENDA

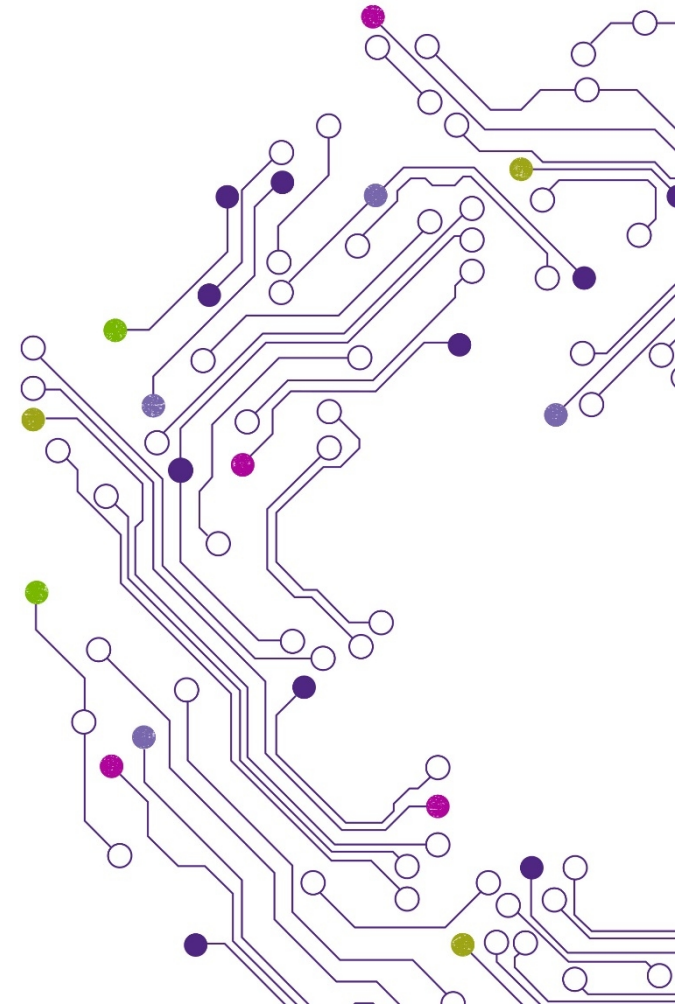
What should companies be doing?



Safeguard the organization against cyber threats

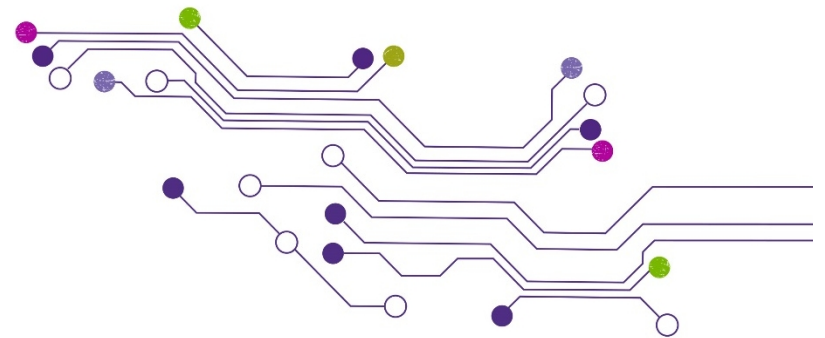
Key actions:

1. Map and classify data
2. Conduct a vulnerability assessment
3. Develop an incident response plan
4. Conduct a vendor assessment
5. Evaluate insurance coverage
6. Stay on top of compliance obligations
7. Create a risk profile
8. Set a cybersecurity risk management strategy



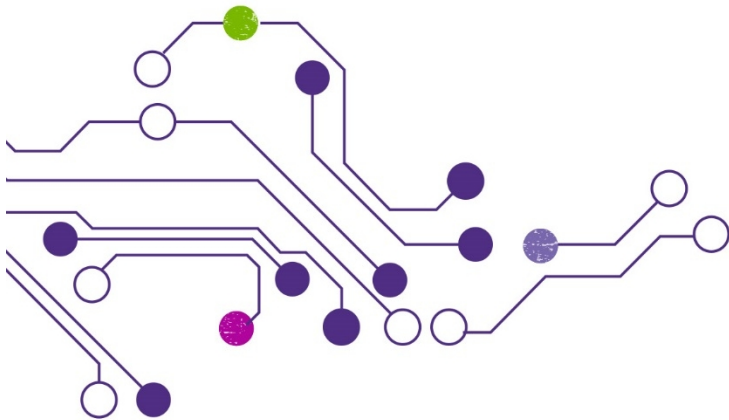
Map and classify data

- Data mapping can help answer important questions like:
 - What are the crown jewels of our business?
 - Is IP important?
 - Are we an information-gathering or data-hosting firm?



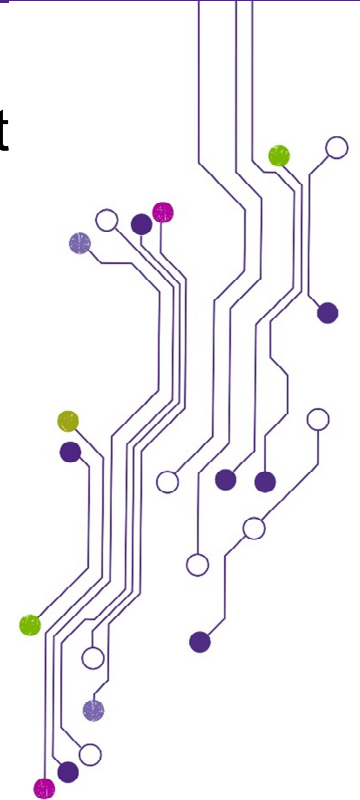
Conduct a vulnerability assessment

- Vulnerability assessments help companies understand what their internal risks are
 - Stay on top of security by performing a penetration test along side of the vulnerability assessment



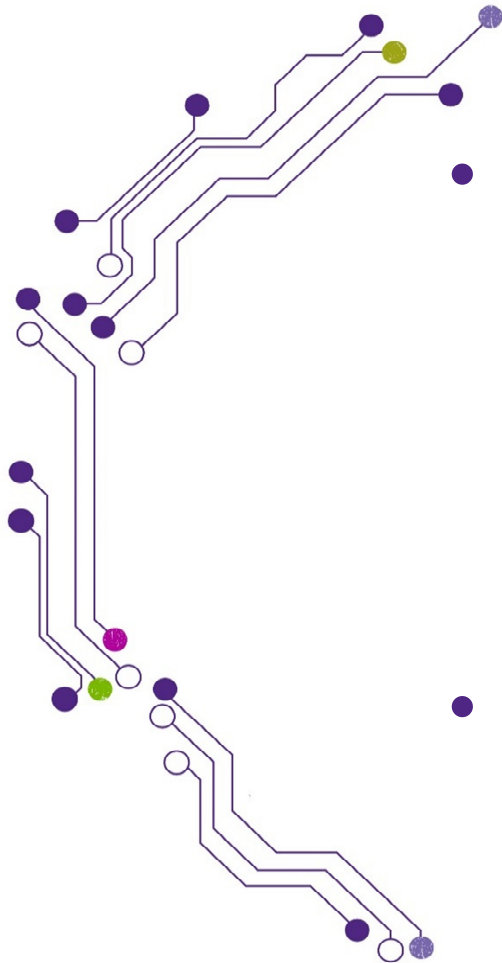
Develop an incident response plan

- Only **4%** of respondents report developing an incident response plan
- An effective response plan is **critical**, and should:
 - Identify specific risk owners and contacts within the organization
 - Have clear decision-making guidelines and associated actions
 - Be usable, and not overly complex
 - Be tested regularly
 - Include all data loss incident types
 - Outline how to help customers



NB: Regular testing of (and improvements to) the plan is crucial.

Conduct a vendor assessment

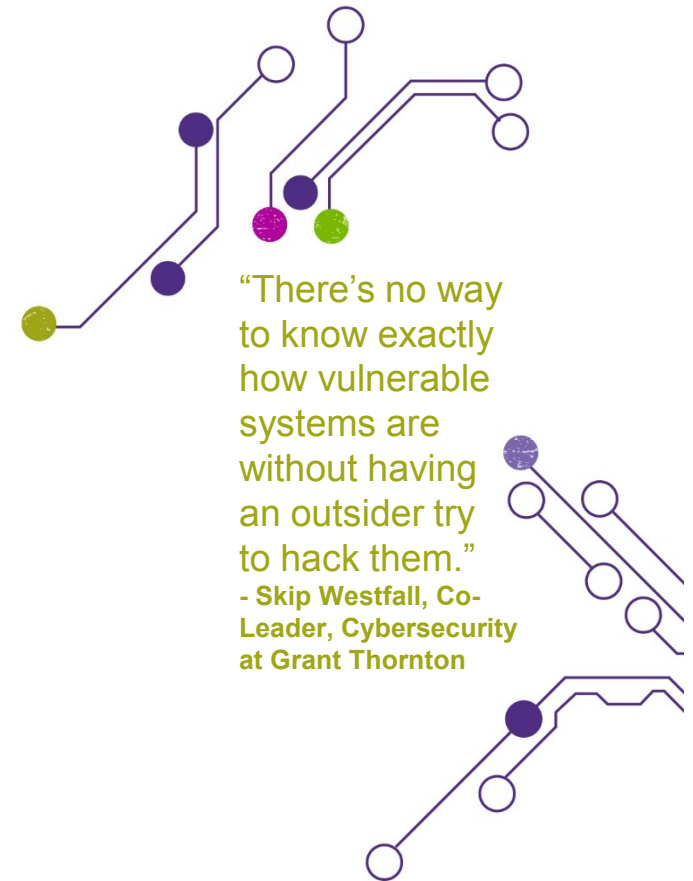


- It's critical to conduct an assessment of vendors' cybersecurity measures **and** assess their vendors' management processes.
- Account for the data held by business partners, vendors and other third parties



Evaluate insurance coverage and stay on top of compliance obligations

- Review insurance policies closely
 - The more costly a breach becomes, the more exclusions insurance companies will include
- Identify glaring vulnerabilities within the risk profile
 - Allocate resources and prioritize which areas to focus on

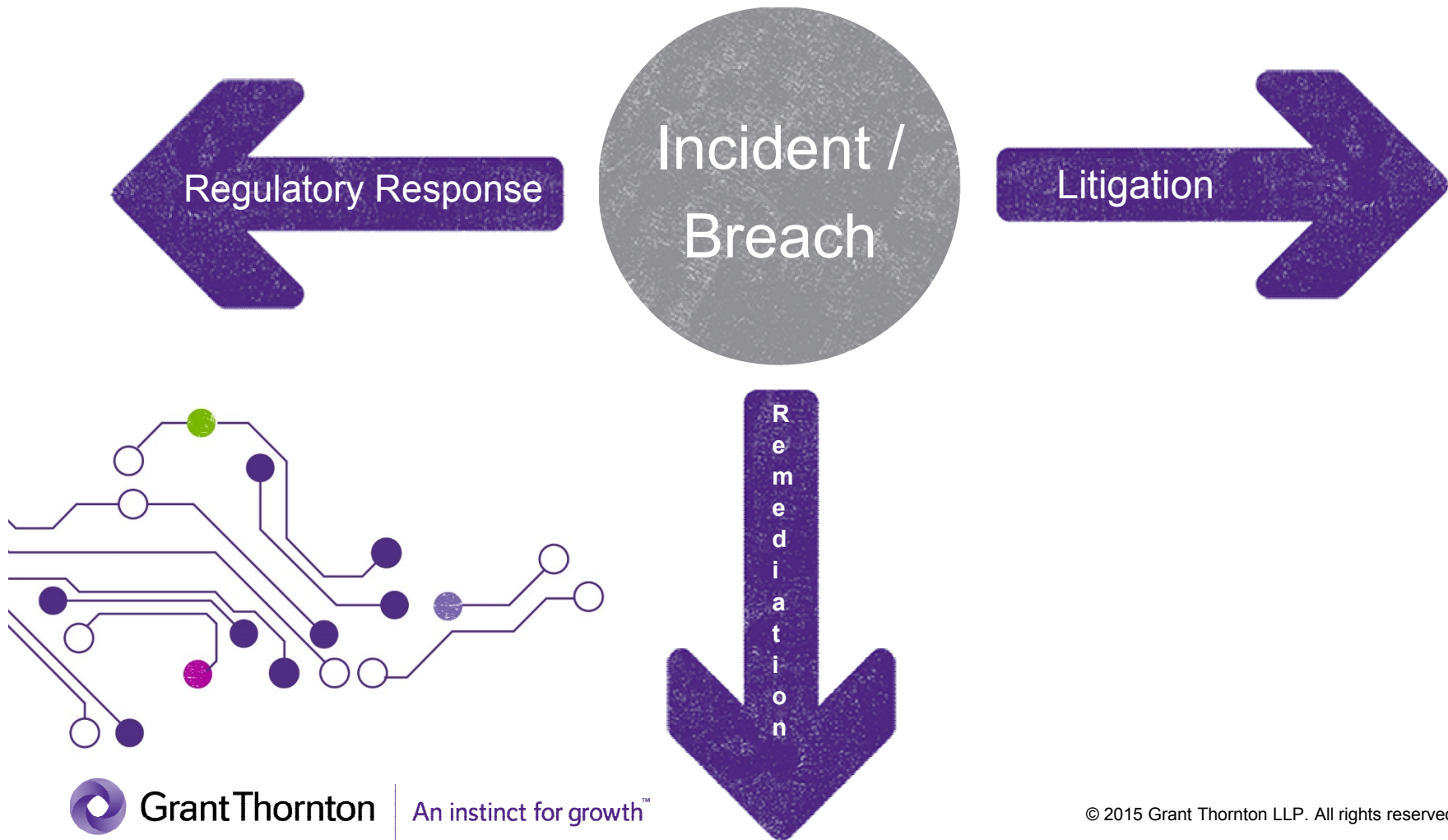


Create a risk profile and set a risk management strategy

- Identify glaring vulnerabilities within the risk profile
 - Allocate resources and prioritize which areas to focus on
- Optimize risk management in three ways:
 - Get directly involved in resourcing
 - Clearly define goals
 - Drive awareness of risks

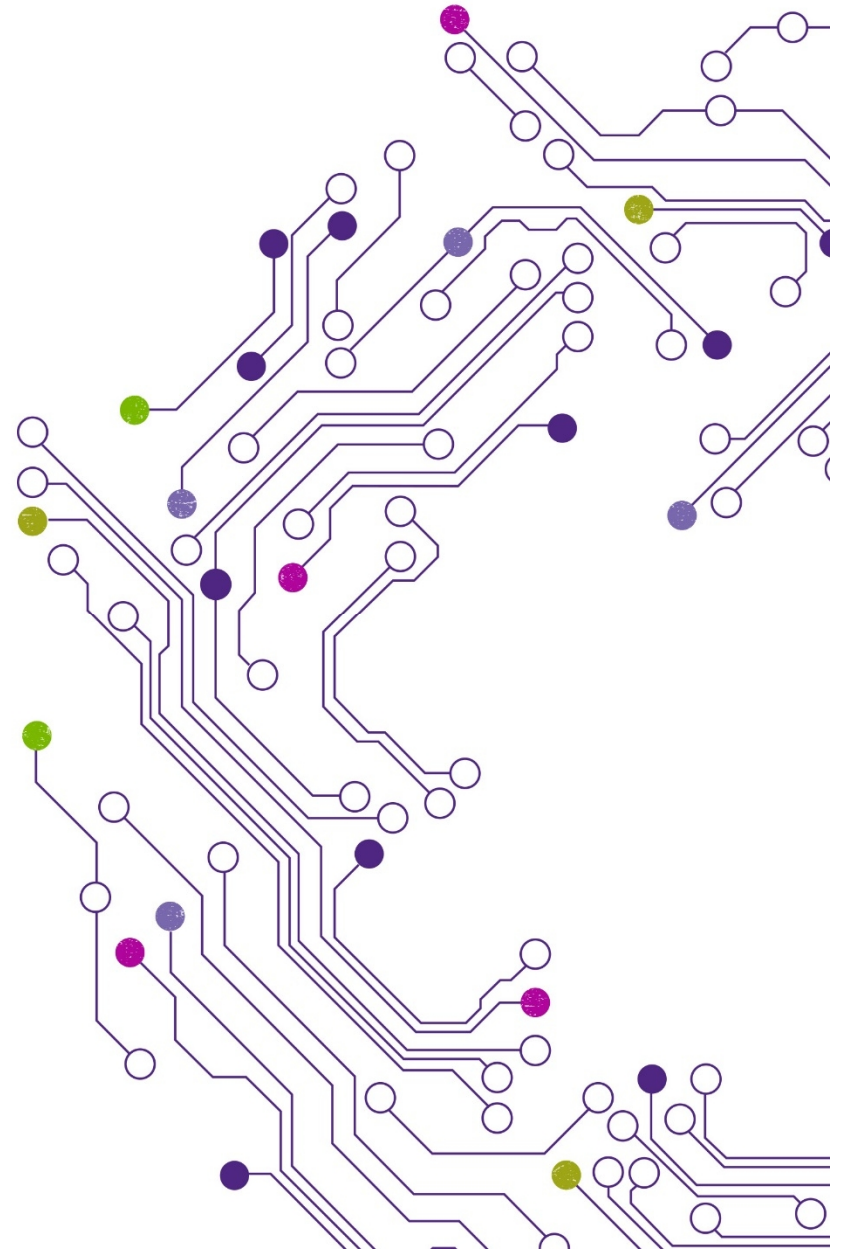


Cover your bases...




AGENDA

What should CFOs be doing?



Establish an effective cybersecurity program

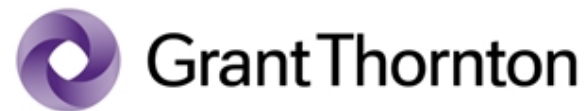
A CFO must take action to assess cybersecurity risks and align your cyber strategy with business strategy:

- 
1. Understand the organization's full risk universe
 2. Advocate for a budget to support cybersecurity preparedness
 3. Develop a close relationship with the CISO or CIO
 4. Know the relevant cybersecurity regulations and SEC expectations
 5. Evaluate the organization's cybersecurity insurance
 6. Report to the board on the cybersecurity initiatives and get buy-in on necessary investments

Comments? Questions?



Thank you



Johnny Lee
Managing Director
Forensic, Investigative & Dispute Services

W: 404.704.0144
M: 404.692.0817
E: J.Lee@us.gt.com

Grant Thornton LLP
U.S. Member Firm of Grant Thornton International Ltd.

Audit • Tax • Advisory

Grant Thornton LLP
1100 Peachtree Street NE, Suite 1200
Atlanta, GA 30309-4504

www.GrantThornton.com