Jamie Rees
@securees
linkedin.com/in/jamierees/

MIND THE GAP

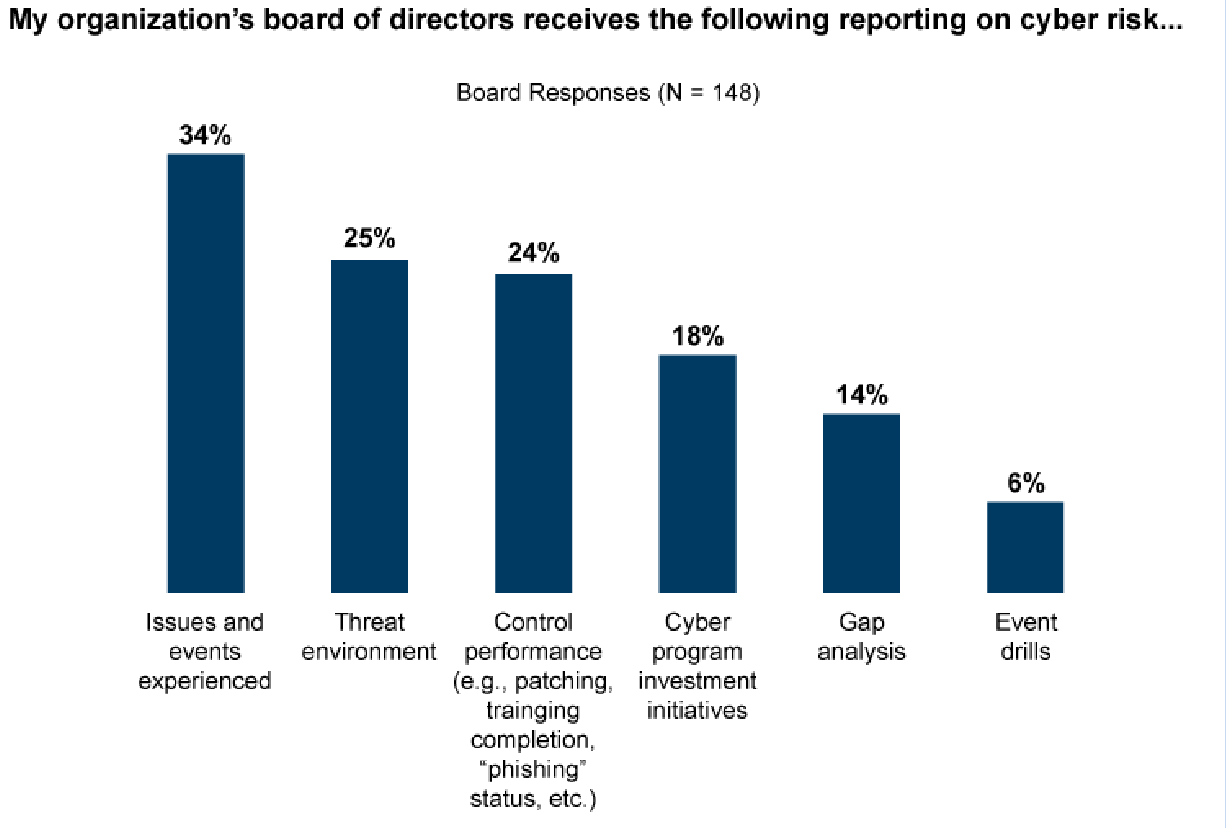
Duty of Care:

“Exercise the care, diligence and skill of a reasonably prudent person in comparable circumstances.”

have the benefit of the business judgment rule and the benefit of an expert reliance defence.[1]

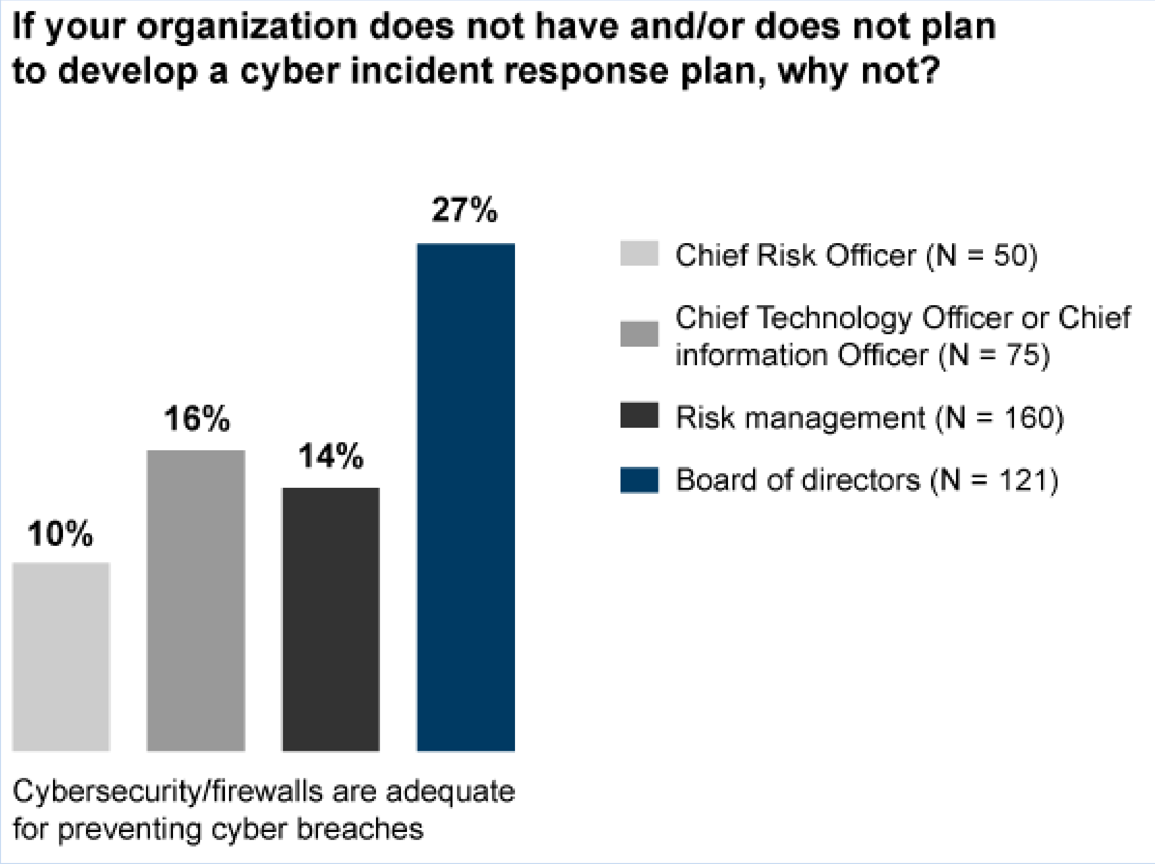
59% report that they find it challenging to oversee cyber risk, and only 19% of respondents report that their boards possess a high level of knowledge about cybersecurity.

National Association of Corporate Directors (NACD) 2


My organization's board of directors receives the following reporting on cyber risk...
Board Responses (N = 148)
34%
25%
24%
18%
14%
6%
Issues and events experienced
Threat environment
Control performance (e.g., patching, trainging completion, "phishing" status, etc.)
Cyber program investment initiatives
Gap analysis
Event drills

National Association of Corporate Directors (NACD)3

Fewer than one-in-five corporate directors say they received cybersecurity investment related information – mostly they get info of past events.

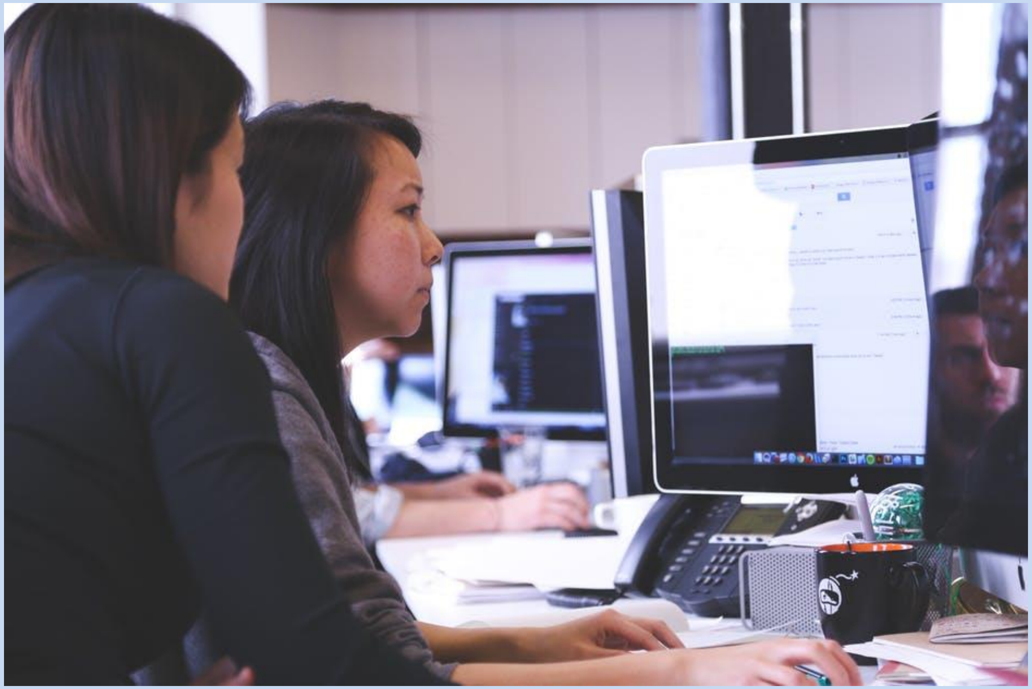

If your organization does not have and/or does not plan to develop a cyber incident response plan, why not?
10%
16%
14%
27%
Chief Risk Officer (N = 50)
Chief Technology Officer or Chief information Officer (N = 75)
Risk management (N = 160)
Board of directors (N = 121)
Cybersecurity/firewalls are adequate for preventing cyber breaches

National Association of Corporate Directors (NACD)3

Have we thought about the impact specific cyber-events can have and whether management's response plan is oriented properly and supported sufficiently?

Are we proactively and periodically evaluating and testing the plan to determine its effectiveness?

Is there someone on the board, or advising the board, who is the point person this topic?



Does the board receive key metrics or reporting that present the current state of the security program in an objective manner?

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.

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

Cybersecurity What The Board Of Directors Needs To Ask IIARF Research Report

There are two major activities to monitor: (i) the build-out and installation of the strategic plan and (ii) the effectiveness of the plan.

The utilization of dashboards to monitor the installation and effectiveness of the strategic plans is essential for meaningful board oversight of cybersecurity strategy. Denton’s: A cybersecurity guide for directors

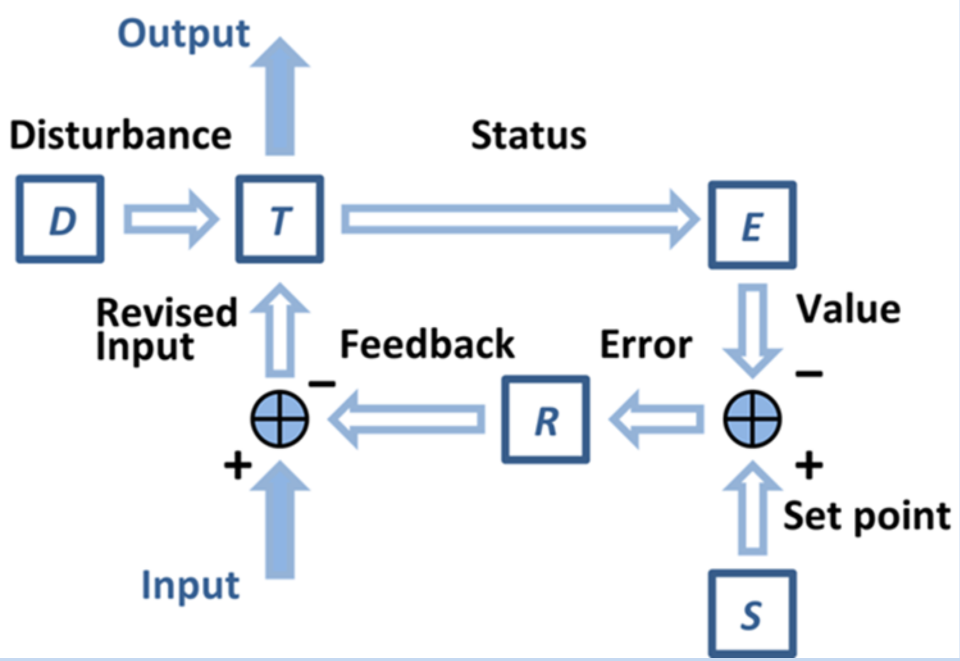
Goal: Build a Cybersecurity Capability that also meets the boards needs. Tell them about it.

Capability: Combination of values, processes and resources.

From least to most flexible, and most to least impactful on a capability's success. Clayton Christensen The Innovator's Dilemma

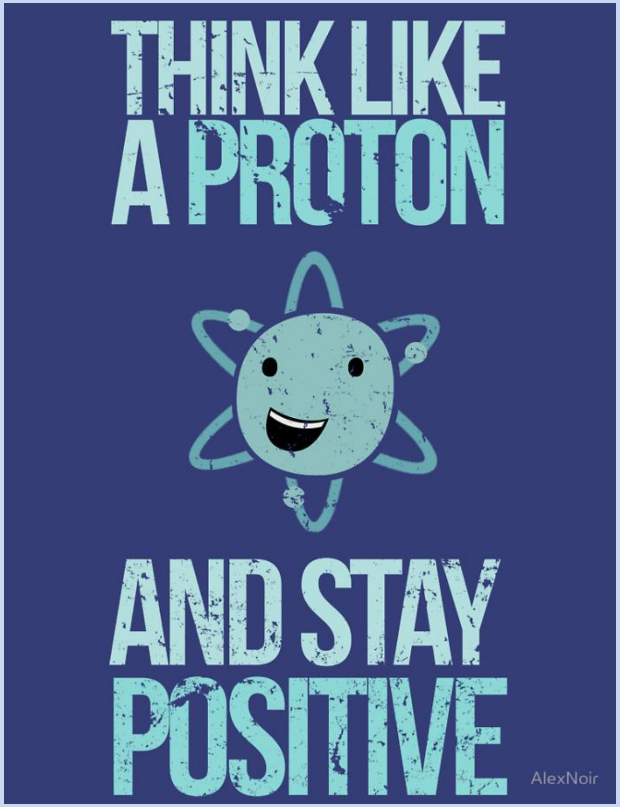
Cybernetics: The study of the control of systems by using feedback 1940s Norbert Wiener

- Halting or reversing disorder
- Human/machine relationship
- Sensors for performance input

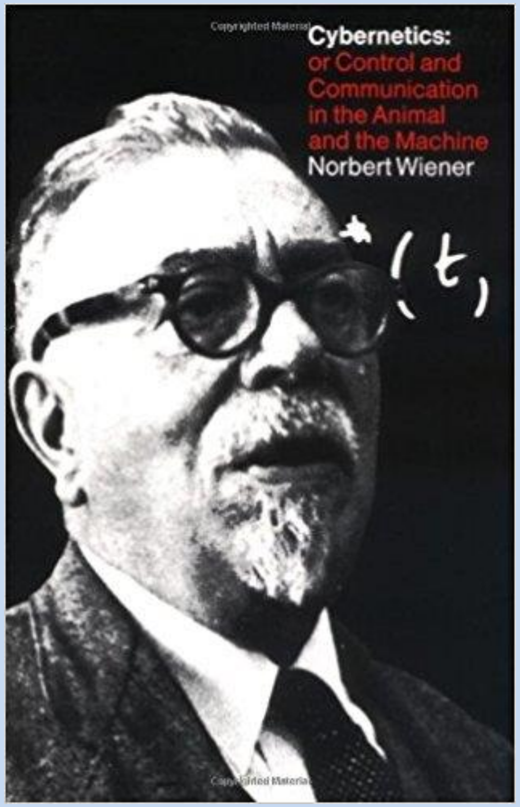


System: A set of *things working together as parts* of a mechanism or an interconnecting network; a complex whole (Oxford)

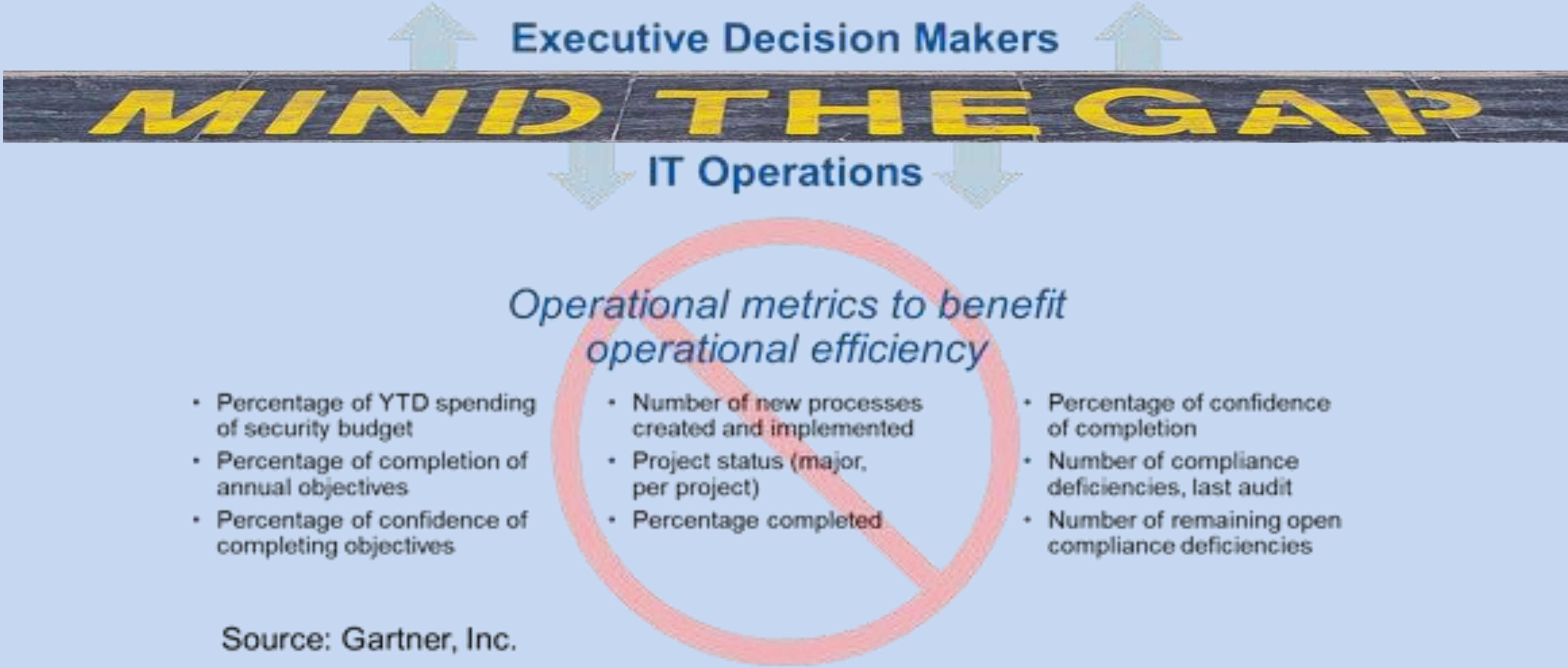
1. Believe



2. HMI



3. Sensors



Executive Decision Makers

IT Operations

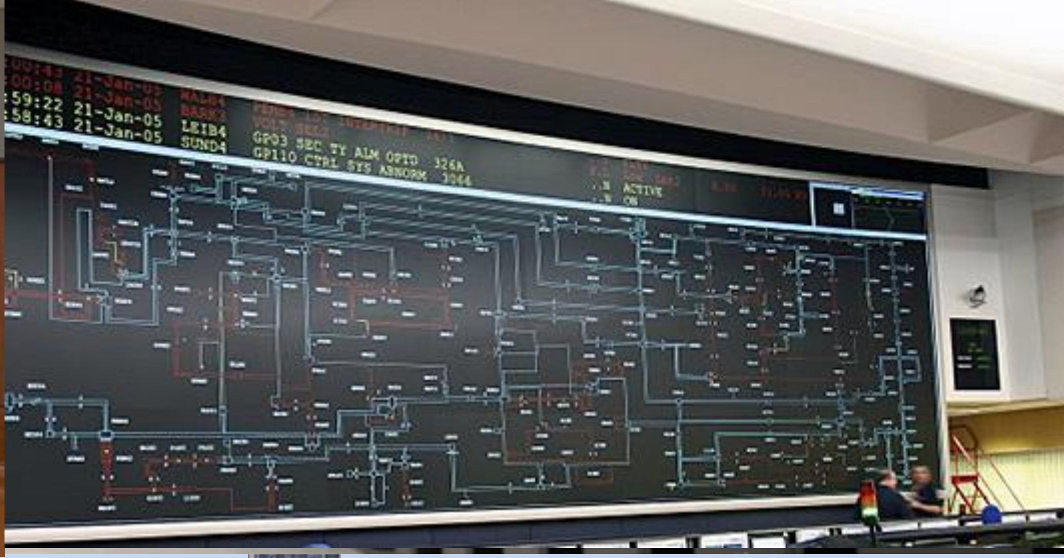
Operational metrics to benefit operational efficiency

- Percentage of YTD spending of security budget
- Percentage of completion of annual objectives
- Percentage of confidence of completing objectives

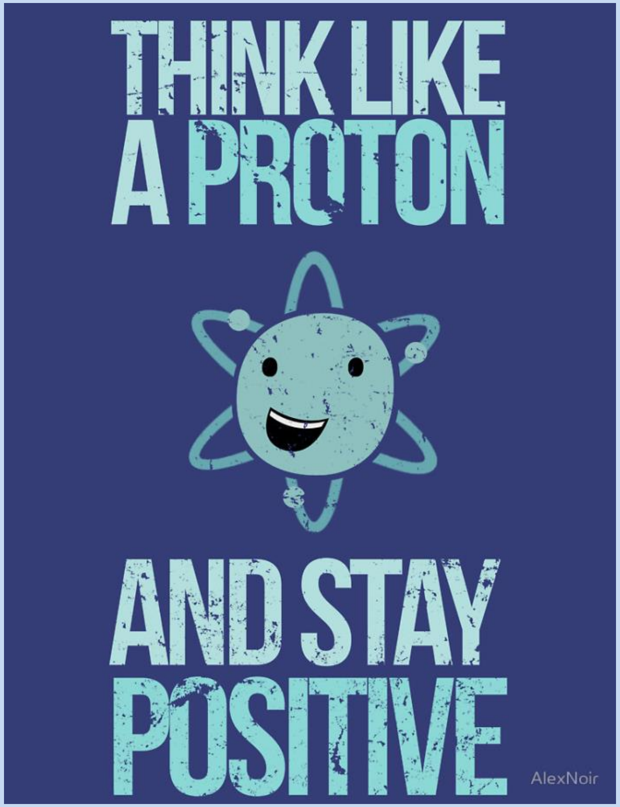
- Number of new processes created and implemented
- Project status (major, per project)
- Percentage completed

- Percentage of confidence of completion
- Number of compliance deficiencies, last audit
- Number of remaining open compliance deficiencies

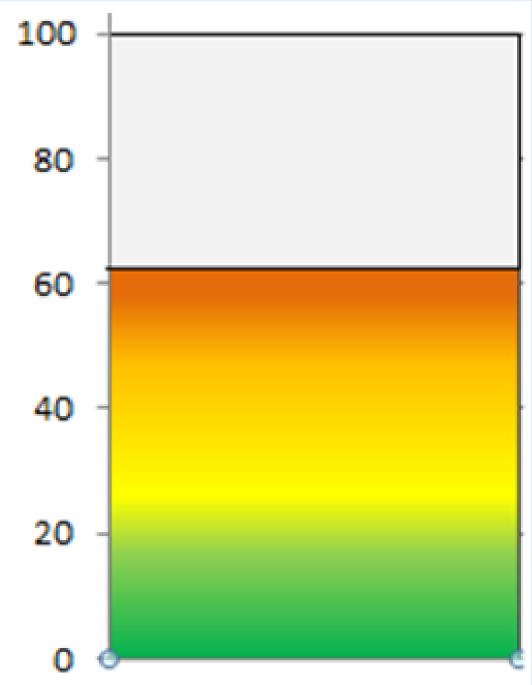
Source: Gartner, Inc.



1. Believe



2. HMI



Cybersecurity
Risk Index

3. Sensors

- Audit Findings
- Vulnerability Management
- Red Team Reports
- Human Element
- SIEM Output
- Threat Intelligence
- Exercise Output
- Insurance

https://www.icd.ca/getmedia/581897ca-d69d-4d4f-a2a2-ca6b06ef223b/5467_Osler_Directors_Responsibilities_Canada-FINAL.pdf.aspx

https://blog.nacdonline.org/2017/03/pubco-survey-transformation/

https://blog.nacdonline.org/2017/04/cyber-risk-oversight-questions/

https://blog.nacdonline.org/2017/11/align-on-cybersecurity/

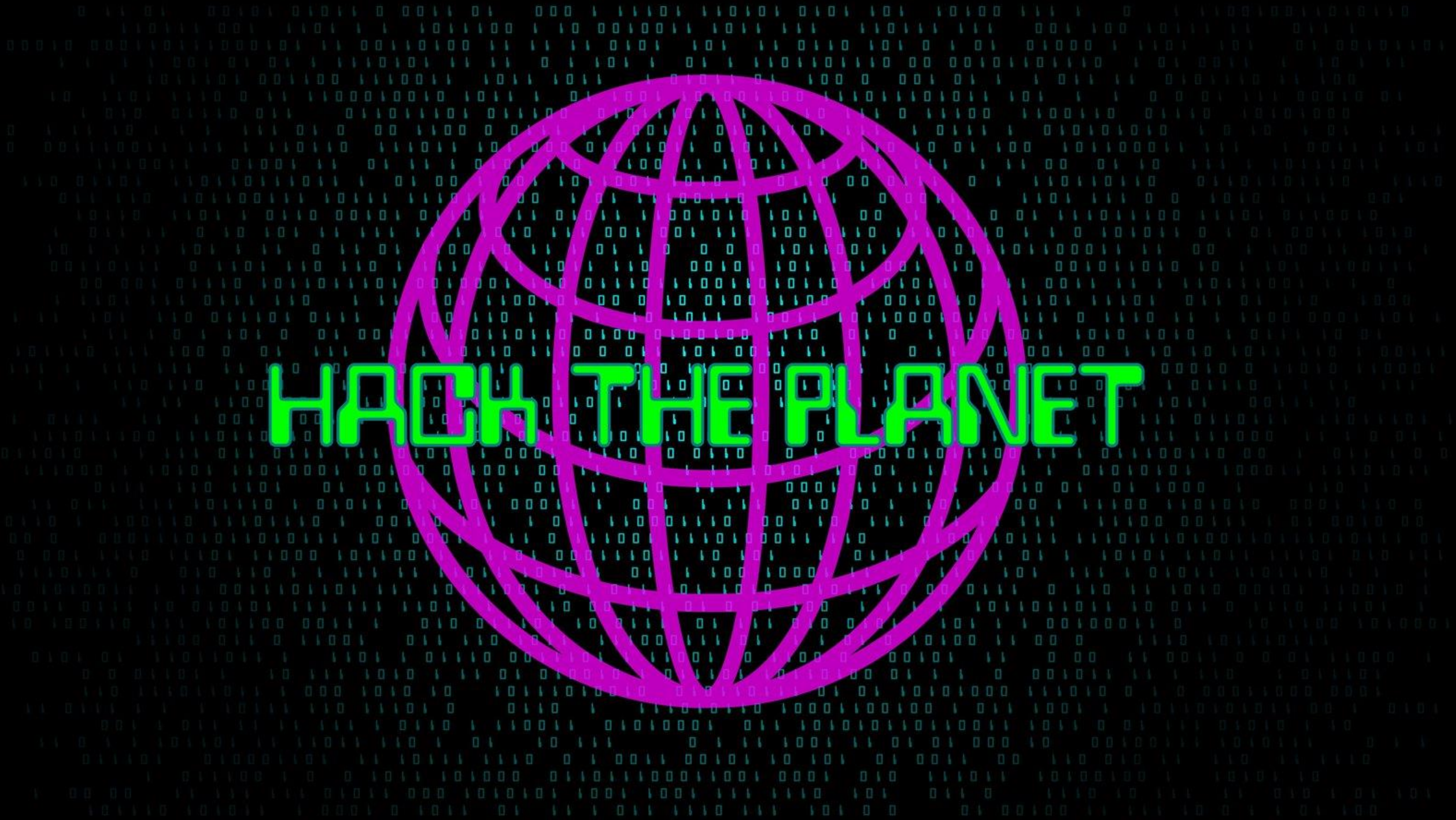
https://corpgov.law.harvard.edu/2017/06/27/ten-questions-every-board-should-ask-in-overseeing-cyber-risks/?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3B1M%2FJSzkaSOGn1u6QFdNCow%3D%3D

https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2015/november/3/a-cybersecurity-guide-for-directors

https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx

http://blogs.gartner.com/paul-proctor/2013/08/11/no-one-cares-about-your-security-metrics-and-you-are-to-blame/

Gartner case study G00270786 Paul Proctor


HACK THE PLANET