Insecure and Disconnected

Cyber attacks often result from a misalignment in cybersecurity behaviors between organizations, departments and employees.

How will organizations solve this complex puzzle?

Employees are Leaking Data

Insiders are the top cause of data breaches. Employees realize data theft is a big issue, but they don't see their piece of the puzzle.

Only a third of employees protect personal information in daily life and are aware of information security at work.[1]

45% of employees say that it's safe to open any email on their work computer.[2]

61% of employees completed cybersecurity training only because it was required by their companies.[2]

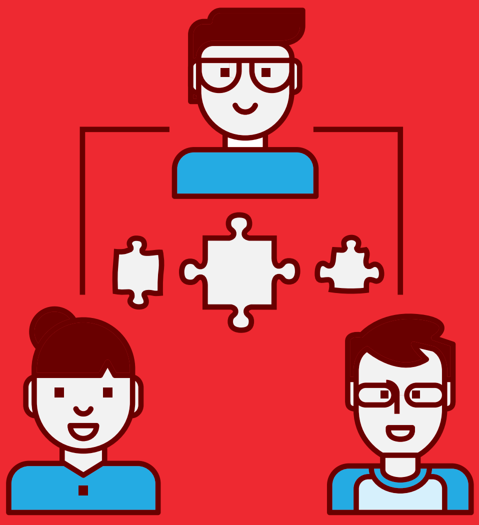
77% of companies believe insufficient employee understanding of cyber risks is a barrier to effectively managing the threat.[2]

Enterprise cybersecurity monitoring policies have yet to win over reluctant employees:

75% say their companies *should* monitor data sources such as emails, telephone calls or messaging services, and yet **89%** still consider this monitoring a violation of their privacy.[3]

Security Policies are Misaligned

Efforts to elevate the organization's approach to cybersecurity — its maturity, resilience and capabilities — can be undermined by a puzzling lack of board agreement or executive support.



Confusion about who's in charge:

81% of CEOs say they're most accountable, while

78% of technical executives make the same claim.[4]

89% of firms don't evaluate the financial impact of big breaches.[2]

24% of CEOs are unaware of a security breach.[4]

90% of organizations have a cybersecurity strategy while

<1/2 **less than half** have fully implemented it.[5]

Toward Cybersecurity Resilience

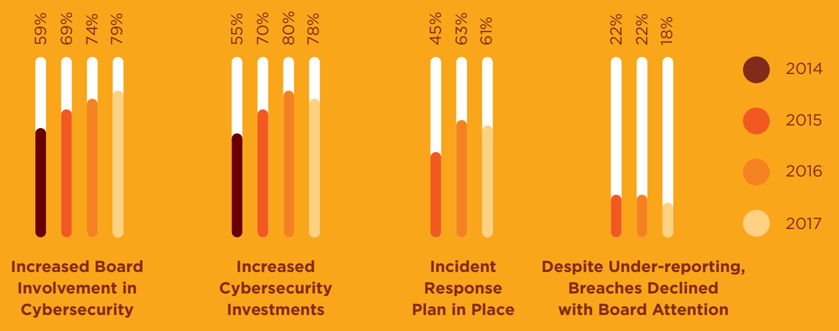
The complexity of aligning your employees, executives and board on an effective cybersecurity program requires everyone to embrace enterprise risk reduction.

The Path to Resiliency:

- Determine your organization's risk-based maturity for capabilities that address organizational risk.
- Gauge if your security program is tailored appropriately for the risk the organization will encounter.
- Develop a risk mitigation roadmap.
- Communicate policies in a transparent matter.
- Explain to everyone how personal behavior can adversely affect corporate security.
- Inform board directors and senior execs of priorities, gaps, roadmap and investment models — in understandable language.

Board Involvement Makes Organizations Safer

High-level involvement in cybersecurity results in greater investment, increased ability to respond to attacks and fewer data breaches.[6]



[1] ISACA http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/Survey-Strong-Tech-Governance-Drives-Improved-Business-Outcomes.aspx

[2] Willis Towers 2017 Watson Cyber Risk Surveys https://www.willistowerswatson.com/en/insights/2017/10/empowered-employees-the-frontline-against-cyber-threats

[3] Ernst & Young 2017 Fraud Survey https://fraudsurveys.ey.com/ey-emeia-fraud-survey-2017/monitoring-data-to-understand-employee-behavior/

[4] Centrify Study http://www.kuam.com/story/37555346/centrify-study-finds-ceo-disconnect-is-weakening-cybersecurity

[5] Cyber Security Trends Survey https://www.herjavecgroup.com/wp-content/uploads/2017/06/Cybersecurity-trends-2017-survey-report.pdf

[6] https://www.bdo.com/insights/assurance/corporate-governance/2017-bdo-board-survey/2017-bdo-cyber-governance-survey

CMMI® Institute