BETTER TECH GOVERNANCE IS BETTER FOR BUSINESS

AN ISACA RESEARCH REPORT

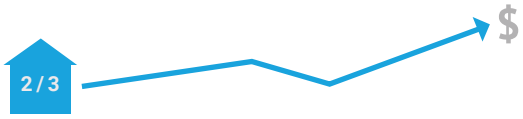
ISACA®

Non-stop cyber-threats and ongoing digital transformation of business have elevated governance of technology into boardrooms across the globe. How are senior leaders handling their growing responsibility for effective oversight of all things digital?

To better understand the issues, attitudes, and actions, ISACA conducted a worldwide survey in the summer of 2017 of 732 board members, C-suite executives, managers, and professionals in a wide range of industries and company sizes. Key findings suggest mixed success in translating heightened recognition of the importance of technology governance into effective action.

On the plus side:

- 9 in 10 senior leaders surveyed agree that better governance of information technology leads to better economic outcomes and more business agility.



- Two-thirds of organizations polled have increased spending on risk management in the past year.

Less favorably:

- More than two-thirds of all respondents say their company's top leaders need to prioritize strengthening connections between IT and business goals.

- Barely more than half agree that their boards and executive teams are doing all they can to safeguard the organization's digital assets.

These disconnects and other findings in this research suggest a "governance gap" is developing – just as the fast-moving business landscape makes it more crucial than ever for organizations to implement effective policies, controls and best practices that maximize technology benefits and minimize risks.

How can organizations use the significant power and influence of top leadership to more effectively leverage technology? This research identifies valuable actions and priorities for successfully navigating the transition to stronger corporate governance of technology.

Hopeful New Captains of the IT Vessel

ISACA and others have long promoted governance as a critical way to manage IT resources, performance, and risk. Success stories of improved business-IT alignment at Grupo Bancolombia and GlaxoSmithKline freeing IT resources for the most productive projects fueled worldwide interest in senior executives establishing strategies, structures and measurements to boost business results.

Now, after years of being perceived mostly as an IT concern, governance has advanced to a board-level issue. Among the many reasons, failure of many tech investments to deliver business returns, the expanding cyber attack surface accelerated by a proliferation of connected devices, and intense new focus on regulatory and audit compliance created by a complex new technology challenges.

Today, belief that better corporate IT governance is good for business has become nearly universal among executives, the ISACA survey shows (Figure 1).

Strong Belief in Governance (Figure 1)

Leadership teams agree that better IT governance leads to two things in particular:

Source: ISACA 2017 Better Tech Governance Is Better for Business Research

Senior leaders express belief that better governance of technology will help their organizations run more leanly and efficiently, become more responsive to customers and partners, and better link spending to demonstrable ROI.

Many also strongly agree that better governance makes organizations more agile. Enabling mobility, using cloud-based services and applications, better targeting and personalizing marketing, and effectively using big data and analytics to make faster and better business decisions all are powerful ways to quickly respond to or create new market opportunities.

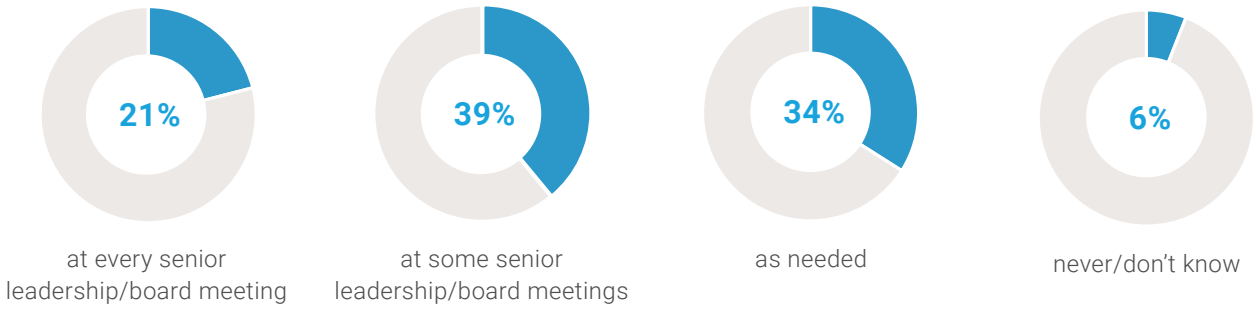
Executive optimism is backed by ample industry evidence. According to Cognizant, an IT consulting firm, effective IT governance maximizes a company's business value in several measurable ways—from better project prioritization to improved performance and higher quality IT output.

Tyro Payments Ltd, a Sydney, Australia-based financial technology company that has been responsible for AUS $36.8 billion in transactions, is a case in point. Technology and governance have been fully embedded into the business since the company's launch in 2003. The company uses agile development techniques, built a core banking platform (for which it was granted an unrestricted banking license,) and tracks cyber security and enterprise risk management issues through a management risk committee.

The Tyro case is replicated throughout the globe. A new research paper by MIT and The Swiss Finance Institute found that share prices of better-governed public companies were 5% higher than those with weaker controls.

Boards in the Know (Figure 2)

How often is your senior leadership briefed about risk topics such as cyber security and disaster recovery/business continuity?



Source: ISACA 2017 Better Tech Governance Is Better for Business Research

The good news is that advocates of strong technology governance now have seemingly enthusiastic allies in high places. They will be needed. The ISACA research revealed two important areas of concern widely voiced across all industries, including other studies.

First is the poor IT and business alignment that stubbornly persists in many organizations. Some 69% of ISACA survey respondents say leadership and boards should make establishing a clear link between the two a top priority. The second is cyber threats.

Cyber Security Job #1

More than anything, cyber security has put governance of technology on the board agenda.

According to the FBI, U.S. financial loss from cybercrime exceeded US $1.3 billion in 2016. Worldwide, data breaches and other attacks will cost businesses $2.1 trillion by 2019, projects Juniper Research, a four-fold increase since 2015. Experts say only about 15% of cybercrime is reported, so actual losses are surely much higher.

Leaders understand that the same hyper-connected environment that enables boundless opportunity also presents a major source of risk that threatens profitability and even survival. Prominent cyber attacks such as WannaCry in May, Petya in June, and Equifax in September raised awareness and fears worldwide.

The business-damaging, career-ending potential of such attacks is not lost on senior leadership. Asked about the top corporate governance technological challenge and opportunity faced by senior leaders, 44% of survey respondents named cyber security policies and defenses, followed closely by risk management (Figure 3).

Top Governance Challenges and Opportunities (Figure 3)

Top 3 most significant governance challenges in the next 12 months.

Answer Choices	%
Cyber security policies and defenses	44%
Risk management priorities	36%
Alignment between IT objectives and overall enterprise objectives	35%

Note: Up to three choices allowed
Source: ISACA 2017 Better Tech Governance Is Better for Business Research

Boardroom worries over increased internal and external threats are so great (61%) that almost half (48%) of leadership teams have prioritized investments in cyber-defense improvements over other programs, including digital transformation and cloud. That makes sense; in another recent ISACA survey, 53% of organizations reported an increase in attacks in 2016, with 80% saying it is either “likely” or “very likely” that they will be attacked this year.

Despite these expressions of concern, troubling gaps between executive attitudes and effective actions were voiced clearly by current survey respondents. Only 55% say their organization’s leadership team board is “doing everything it can” to safeguard their organization’s digital assets and data.

Reasons for doubt vary. Only 1 in 3 organizations say they assess risk related to technology use at least monthly.

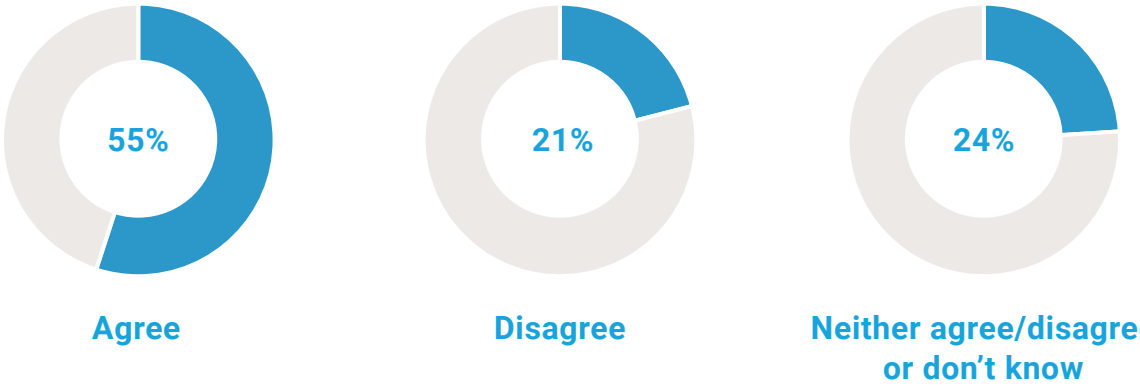
Unfortunately, all signs point to continued escalation of attacks for the foreseeable future. Insiders, hacktivists, criminals, terrorists, and nation states pose a dizzying range of new threats, from cyber-extortion to attacking cloud services and devices connected to the Internet of Things (IoT). Hacking, malware, phishing, social engineering, botnets, and stolen user credentials remain potent dangers.

The connection between cyber security and a company's bottom line is clear to board members — and they're worried, with good cause. A recent British report found that a publicly reported cyber-attack can cause a drop of 15% in company share prices. Such high stakes and pressure from a wide variety of external and internal stakeholders ensure senior leadership teams will continue to make cyber defense a top priority.

One of the key reasons boards must offer strong oversight of cyber security is that it sets the tone for the rest of the organization. An active and engaged board will consider initiatives advocated by cyber security leaders across the organization.

Data Protection (Figure 4)

Do you agree or disagree that your senior leadership or board of directors is doing everything it can to safeguard your organization's digital assets and data records?



Responses have been rounded to the nearest whole number and may not add up to 100 percent.
Source: ISACA 2017 Better Tech Governance Is Better for Business Research

Topping the Governance Agenda

Besides identifying key strategies for improving governance, this research also revealed several areas both respondents and experts say deserve more boardroom attention.

Governance Frameworks

If there's a secret weapon against technology performance gaps, it's governance frameworks.

Adoption of a structured framework like ISACA's COBIT, used by 28% of respondents, provides a proven way for senior leaders to create conditions needed for effective governance: alignment between IT and stakeholders, monitoring and metrics, and strong engagement by business units and tech leaders (Figure 5).

Success Factors (Figure 5)

Which conditions must be present for senior leadership to demonstrate effective IT governance?

Answer Choices	%
Ensuring alignment between IT and stakeholder needs	58%
Monitoring and measuring results toward goals	39%
Strong Chairman, CEO or executive guidance	33%
Strong engagement by business units, employees	30%
CIO and/or CISO should be on the board	23%
Prioritizing financial investment in governance	20%
Utilizing appropriate frameworks	19%

Note: Up to three choices allowed
Source: ISACA 2017 Better Tech Governance Is Better for Business Research

Frameworks also short-circuit the most-oft cited governance weaknesses: Infrequent board briefings on risk topics (only 21% do so at every meeting) and spotty risk assessment (only one-third do monthly).

Fortunately, most organizations surveyed already use governance frameworks. However, for many, there's some disconnect between widespread adoption and results. That suggests the need to deepen commitment and continue training with certified experts who can help organizations and boards get maximum benefit from these powerful tools.

Compliance

Besides identifying key strategies for improving governance, this research also revealed several areas both respondents and experts say deserve more boardroom attention.

As new cyber security and privacy rules come into force worldwide, strategic consultants advise corporate directors and leaders to reassess how they exercise their governance responsibilities for handling cyber risk and compliance. For those boards that do business globally but need a stronger incentive, EU General Data Protection Regulation (GDPR) looms largest. Effective May 2018, the law mandates a 72-hour breach notification, appointment of a company Data Protection Officer, and major fines for mishandled data.

Of concern, only 32% of companies affected are satisfied with the progress they've made to prepare for GDPR, the ISACA research found. More than one third (35%) of respondents are unsure of the progress their organization has made to prepare for GDPR. There's hope for improvement; a recent PwC survey found more than half of US. multinationals consider GDPR their top data protection priority, with 77% planning to spend more than $1 million or more.

Security Training

Topping the priority list in some organizations is data security training. More than 1 in 3 (35%) respondents intend to increase budgets for employee awareness and skills education. The security training investment often ranges from $1,000- $2,500 per person, another ISACA survey found.

More companies may boost their security training allocations if the proposed US Cyber Security Disclosure Act of 2017 passes Congress, because it requires at least one board member of a public company to be expert in security, or explain why other new measures make doing so unnecessary. Our survey found a small (15%) but undoubtedly leading-edge number of respondents investing more money in training board members on a variety of security issues.

Strategic Investing

Strong board oversight is critical in ensuring investments in people and equipment strategically align with enterprise goals. By that standard, the ISACA survey signals good news. Some 64% are prioritizing and increasing funding for enterprise cyber security and risk-related programs for next year; 25% are investing in upgrading perimeter defense.

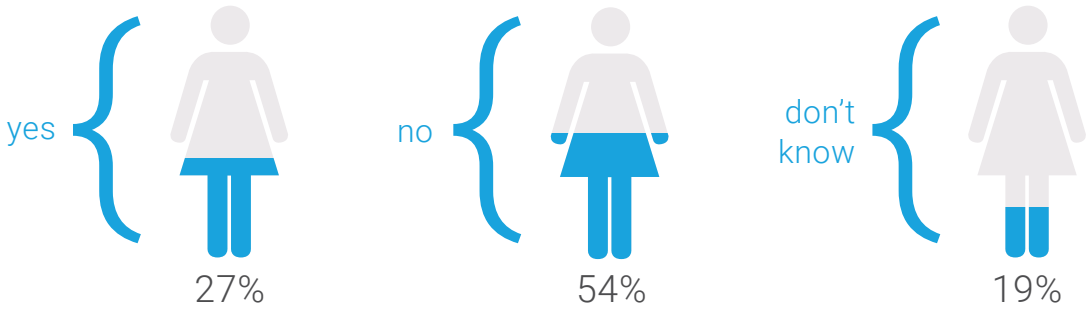
Hire Women

To better meet the technology-driven challenges they face, organizations need to draw upon a more robust workforce. For many, that means hiring and training more women. In this regard, many companies surveyed are, unfortunately, lacking. Only 27% reported an increase in female technology workers over last year. (Figure 6)

Spencer Stuart reports that only 20% of S&P 500 board members are women, so bringing in more qualified tech workers, especially in security, will require company-wide commitment from all. In the ISACA research, only 42% of respondents say that women are equally represented in senior levels at their organization.

Hiring More Female Tech Workers (Figure 6)

Are there more female technology employees in your organization this year than there were one year ago?



Source: ISACA 2017 Better Tech Governance Is Better for Business Research

Next Steps

Better governance helps organizations maximize benefits and minimize risks in a fast-changing technology environment. To be effective, strong awareness and appreciation by top leadership must be converted into focused, meaningful action. Organizations must prioritize recruiting of tech-savvy board members and executives, while continually ensuring that technology priorities and investments are better aligned to overall enterprise strategy. Good foundational work has begun, but ongoing effort is needed to translate awareness into real business benefits and secure environments.

"The boardroom must become hyper-vigilant in ensuring a tight linkage between business goals and IT goals, fully leveraging business technology to improve business outcomes while diligently safeguarding the organization's digital assets," said Matt Loeb, CEO of ISACA. "The message from our research is clear: there is much work to do in information and technology governance. Committing to a boardroom with technology savvy and experience strongly represented provides the needed foundation for organizations to effectively and securely innovate through technology."

- Analyze enterprise risks if security budget shrinks
- Ensure tech expertise is represented in boardroom
- Conduct continuous security awareness training
- Align tech investments with enterprise strategy
- Research and employ industry best practices and security controls

About ISACA's Better Tech Governance Is Better for Business Research

Believed to be the first of its kind in the industry, the online survey of ISACA members was conducted in the summer of 2017 and included 732 respondents from 87 countries spanning Africa, Asia, Europe, Latin American, Middle East, North America, and Oceania. Respondents all hold leadership roles with working knowledge of how their organization's senior leadership and/or board of directors decides its IT strategy, plans or governance. The majority of respondents hold titles of CEO, CIO, CTO, CISO, CSO, Executive VP, Security Executive, Executive Manager, General Auditor, Partner, and Audit Head. Respondents' organizations spanned government, military and a range of industries including financial/banking, technology services, manufacturing/engineering, health care/medical, insurance and retail.