2019 Cyber Security Teams Survey Report

The CISO Challenge:

Aligning Business Enablement with Enforcement

New survey highlights internal management issues facing IT cyber security teams in Europe

thycotic

EXECUTIVE SUMMARY

2019 Cyber Security Teams Survey Report

CISOs Must Manage Up to Executive Boards and Across to All Employees

Research among IT security execs in UK and Germany highlights internal challenges

It seems as if every week we get news about a new cyber security data breach, whether it is among Facebook users, MyFitnessPal members or Marriott hotel guests. And with each incident, we are reminded of how cyber security must become an integral part of daily operations in order to properly protect and secure information for our customers, employees and businesses.

As the traditional boundaries disappear in an always on, Internet connected world, more organizations than ever recognize the need for cyber security to take on a major management role—often with a designated individual in the position of Chief Information Security Officer or CISO.

To help CISOs understand their pivotal and evolving role as management leaders, Thycotic conducted research to determine how IT security is perceived among 200 organizations in the UK and Germany. Survey respondents included cyber security decision makers from diverse industries including IT and telecommunications, financial services, public sector, manufacturing, retail, transportation and more. All organizations surveyed had more than 1000 employees with almost 30 percent of those surveyed organizations employed more than 5000 people.

70%

of respondents indicated they have "full responsibility" for their organization's cyber security efforts.

49.5%

of surveyed organizations have the CISO position serving on their executive boards.

35.5%

still do not include the CISO as a key member of the executive management team.

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

Here are Research Key Takeaways

#1
Key Takeaway

Executive board perceptions restrict cyber security effectiveness.

#2
Key Takeaway

While executives may say cyber security is a priority, they need to follow through with strategic investments.

#3
Key Takeaway

Cyber security must be made more visible and a positive experience for all employees and departments.

Survey Results

What involvement do you have with your organization's IT security?

	Total	UK	Germany
I am fully responsible	**72%**	68%	76%
I have some responsibility	**28%**	32%	24%

In your company does the CISO have a place on the board?

	Total	UK	Germany
Yes	**49.5%**	41%	58%
No, but they should do	**35.5%**	38%	33%
No, and they're correct not to	**5%**	6%	4%
We do not have CISO	**6%**	8%	4%
Don't know	**4%**	7%	1%

Given the enormous impact of security breaches on companies and the increase in regulations on data privacy, this report helps identify key internal management issues facing those individuals most responsible for the cyber security of their organizations. But as the results of the survey suggest, that responsibility must be acknowledged and shared by executive boards as well as all employees if organizations are to be properly protected from threats that grow more numerous and sophisticated each day.

KEY TAKEAWAY

Executive board perceptions restrict cyber security effectiveness

While cyber security has captured much more attention among executive board members, survey respondents said executive boards generally express passive expectations from their IT security teams. They see the role of the IT security team as "keeping the lights on and systems running." While this is a must for any organization's cyber security efforts, less than a quarter of board members view IT security as an important strategic business enabler. Traditional attitudes about cyber security appear to remain entrenched, with boards seeing IT security as reactive vs. proactive, a cost rather than an asset, a policeman rather than an enabler, and a team that says "No" rather than "How."

Whether or not these perceptions are justified, they can have a powerful negative effect on how well organizations implement and manage cyber security.

Survey Results

Which best describes how you think your organization's board/c-suite currently view the function?

	Total	UK	Germany
Ensuring that nothing bad happens/there are no major security incidents or downtime	**27%**	24%	30%
Protecting customers and employees from security incidents	**25%**	30%	20%
Enabling the business to grow and roll out new services securely	**23%**	24%	22%
Gaining competitive advantage through good data handling	**14%**	13%	15%
Responsible for ticking the 'compliance' box	**8.5%**	8%	9%
Just keeping old antivirus and firewalls running	**2.5%**	1%	4%

Generally, executive boards see the IT security team as ensuring nothing bad happens, with a focus on protecting against cyber security incidents.

50%

believed IT security is all about keeping the lights on and systems working.

9%

saw their role as checking the compliance box.

3%

had a very narrow view of cyber security's job as keeping antivirus and firewalls running.

Only

23%

viewed the IT security role as helping to enable new business and rolling out new services securely.

In your opinion, which best describes how your organization's board/ c-suite perceives how the security team operates?

	Total	UK	Germany
As a positive force for innovation	53.5%	44%	63%
Reactive rather than proactive	36%	41%	31%
As a cost rather than an asset	30.5%	33%	28%
As the 'policemen' rather than enabler	26%	38%	14%
The team that says 'No' rather than 'How'	17.5%	21%	14%
Other (please specify)	1.5%	2%	1%
None of the above	2%	1%	3%
Don't know	0.5%	1%	0%

54%

of respondents indicated the executive board considers IT security as an enabler of technology innovation.

67%

said IT security is viewed either as merely reactive to business needs or a cost rather than an asset to the organization.

26%

found their role defined as security guards rather than business enablers.

17%

said the security team is perceived as saying "No" rather than "How" to executive requests.

Does the perception of the board ever restrict IT security in your organization?

	Total	UK	Germany
Yes, a large restriction	**11.5%**	11%	12%
Yes, somewhat a resistriction	**48.5%**	45%	52%
No restriction	**36.5%**	37%	36%
Don't know	**3.5%**	7%	0%

36%

of respondents said executive board perceptions did not restrict the effectiveness of IT security.

11.5%

said boards had a large negative impact.

50%

indicated board perceptions had at least somewhat of a negative effect on their security efforts.

Recommendations

While information security leaders and CISOs have the responsibility to protect their organization's critical assets and keep the business running, they need to articulate and explore ways to use their knowledge in ways that further the growth of business rather than simply protecting data assets. CISOs should be "managing up" to executive boards from an enterprise risk management viewpoint, assessing the impact of cyber security on their business as a whole.

To be entitled to a position on executive boards, CISOs need to communicate in the vocabulary of business enablers—finding ways to use secure technologies that support revenue and profit initiatives. That means ensuring the tools and policies they implement will both improve their organization's security posture and promote more efficient business processes—adding value beyond just securing the IT infrastructure.

Ultimately, the cyber security team must act more as a "business risk" team, aligned with the business goals and using cyber security skills to reduce business risks that have been accepted and acknowledged by the board. Until both the CISO and the board speak the same language, cyber security will be limited to a reactive role, preventing incidents—lacking the needed security investments that reduce business risks.

Free Resources

How CISOs Can Win a Seat With the Board of Directors

thycotic.com/gartnermarketguide

Cyber security threats are a major concern for Board of Directors which gives CISOs an opportunity to raise their visibility and influence at the highest levels. Find out what it takes to move beyond simply protecting information assets to a larger role in helping to grow your business.

The Forrester Wave™: Privileged Identity Management, Q4 2018 Report

thycotic.com/privileged-access-security-leader/

See why security pros are trusting PIM vendors to become strategic partners. Learn which companies provide cloud and DevOps secret management to deliver effective privilege threat mitigation.

KEY TAKEAWAY

While executives may say cyber security is a priority, they do not always follow through with strategic investments

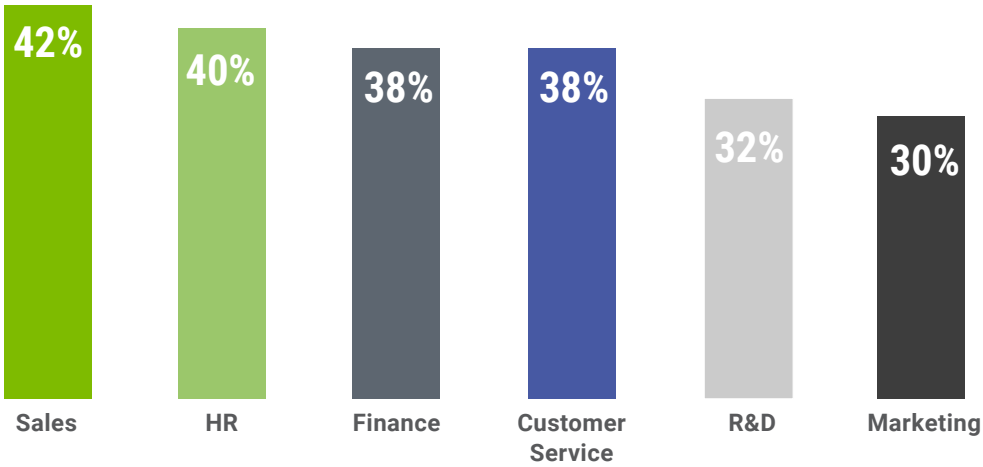
While most IT security leaders surveyed, believe their executive boards listen to them, value their input and understand their importance, they see IT security ranking last in terms of a strategic priority among other business functions such as sales, HR, finance, R&D, and marketing. Nearly two out of three also agree or strongly agree that executive board members don't understand the business case for IT security investments.

It's imperative that CISOs and IT security leaders demonstrate the business value of cyber security to executive boards and their peers in other departments. They need to go beyond the "checkbox" approach of defining cyber security performance only in terms of compliance with regulations and expand their role in assessing and mitigating risk across the entire organization.

Survey Results

Survey respondents indicated IT security is at the bottom of their organization's strategic priorities and sometimes invisible to their executive boards. IT security is perceived as a business function rather than an important strategic priority. Approximately 40% of survey respondents view sales, HR, Finance, customer service, R&D and Marketing as higher business importance. However each of those departments rely on IT security to operate securely.

In your organization do you think that the board considers the below functions to be more or less of a strategic priority when compared to IT security?



To what extent do you agree with the following statements?

I feel that the board listens to us and values our input.

	Total	UK	Germany
Strongly agree	27.5%	24%	31%
Agree	60%	63%	57%
Disagree	10%	12%	8%
Strongly disagree	1%	0%	2%
Don't know	1.5%	1%	2%

The board level can't always see the business case for security investments.

	Total	UK	Germany
Strongly agree	17%	16%	18%
Agree	48%	49%	47%
Disagree	28%	28%	28%
Strongly disagree	6%	6%	6%
Don't know	1%	1%	1%

The board has a good understanding of the strategic importance of the security team within the business.

	Total	UK	Germany
Strongly agree	24.5%	27%	22%
Agree	59%	55%	63%
Disagree	13.5%	17%	10%
Strongly disagree	1.5%	0%	3%
Don't know	1.5%	1%	2%

80%

of IT security leaders said the board had a good understanding of the strategic importance of security investments and values their input.

2 of 3

struggled with getting boards to see the business value in these investments.

65%

agreed or strongly agreed that that boards cannot always see the business case.

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

How does the company you work for measure IT security success?

	Total	UK	Germany
Against how security is benefiting the business overall	55.5%	42%	69%
Against meeting compliance/regulatory requirements	54%	60%	48%
Against how many incidents/attacks are prevented	53.5%	64%	43%
Against specific industry best practices	34%	43%	25%
Other (please specify)	0.5%	1%	0%
We don't currently have measurements in place	2%	4%	0%

55%

indicated the success of cyber security efforts are measured against how they benefit the business overall.

54%

felt success was measured primarily in meeting compliance and regulatory requirements.

53%

said success is measured in preventing incidents and attacks.

Recommendations

Measuring cyber security risk has always been difficult for many organizations, and this remains a challenge for CISOs in showing business value to executive boards. Without risk metrics and a common vocabulary to measure value, CISOs will continue to struggle with gaining strategic relevance and investments for cyber security. If CISOs do not act, perceptions of IT security will remain focused on keeping existing security controls working, making continuous improvements where possible, and improving security technologies that the business has already adopted.

But if IT security leaders are ever to earn a place among executive boards they will need to define the business impact of cyber security and assess business risk with clear metrics. They will need to ensure business resiliency and enable business growth with more efficient and effective cyber security safeguards in daily operations, as well as protect business continuity and mitigate risk with comprehensive incident response and recovery plans.

Free Resources

Privileged Account Management Risk Assessment Tool

thycotic.com/pam-risk-tool

Free online Privileged Account Management (PAM) Risk Assessment Tool.

Privileged Access Management Maturity Model Assessment Tool

thycotic.com/pam-maturity

Free online PAM Maturity Assessment defines four phases of PAM maturity organizations typically progress through as they evolve from laggards to leaders.

KEY TAKEAWAY

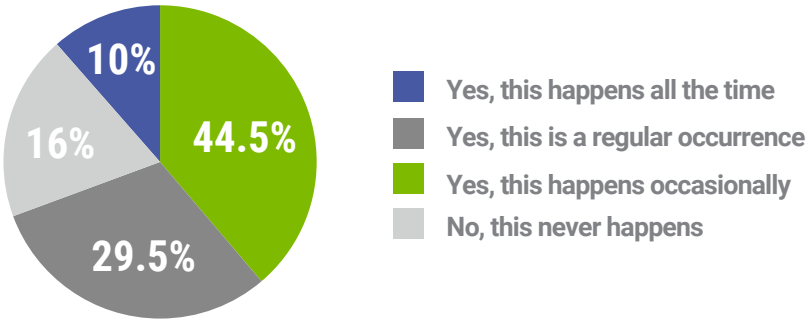
Cyber security must be made more visible and a positive experience for all employees and departments

According to survey respondents, two out of three employees had a negative experience or are indifferent when it comes to cyber security. This may reflect more traditional notions that cyber security can hinder rather than help employees accomplish their jobs—especially when specific actions are blocked or applications unavailable due to security restrictions. Employees also do not get measured on how secure they are but how well they perform their jobs.

IT security leaders and CISOs need to educate managers and employees in all departments about the importance of cyber security and their individual responsibilities in contributing to the cyber health of the entire organization. Entrenched notions of security teams as "fearmongers" must be challenged to gain buy in and support among fellow executives in other functional departments. As organizations start to roll out more Internet of Things (IoT) devices organizations will need to treat cyber security as a safety risk versus an IT risk, future cyber threats can escalate to serious employee risks as IoT devices start to control more critical systems.

Survey Results

Within your organization, have you ever felt that employees (in general) are negative towards IT security staff and their work?



39.5%

of survey respondents felt that employees had a negative impression either all the time or on a regular basis.

44.5%

indicated negative feelings toward the IT security team occasionally.

Only **16%**

did not feel employees had a negative impression of the security team.

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

When your team rolls out a new IT security policy/ introduces new IT security measures that impact employees, what is the typical response from the users?

	Total	UK	Germany
Generally negative-with questions/ feedback that this will hamper their day to day work	**27%**	35%	19%
Generally indifferent-they barely notice	**43%**	39%	47%
Generally positive-we feel our efforts are appreciated	**30%**	26%	34%

30%

of employees appreciate the rollout of new security policies or technologies in their organizations.

27%

still fear the rollout will interfere with their daily tasks.

43%

are generally indifferent or do not notice the rollout—a sign that security measures, if not noticed, are not impacting productivity.

In your opinion, which of the below best describes how employees in your organization view the security team?

	Total	UK	Germany
The good guys: helping them to work safely and securely	**44%**	37%	51%
They don't: we're something that runs in the background which they don't really notice	**26%**	27%	25%
The 'doom-mongers'/ disciplinarians: providing additional layers of process that can slow down their daily tasks	**25%**	30%	20%
A necessary evil	**5%**	6%	4%

On a positive note

44%

felt the IT security team was viewed as, "the good guys" helping to keep the organization safe from threats.

30%

saw themselves viewed as "doom mongers" and a necessary evil.

26%

were indifferent.

To what extent do you agree with the following statements?

Other departments and functions across my company could have a better understanding of what the security team is trying to achieve.

	Total	UK	Germany
Strongly agree	25.5%	26%	25%
Agree	56%	64%	48%
Disagree	15%	10%	20%
Strongly disagree	1.5%	0%	3%
Don't know	2%	0%	4%

It could be easier to communicate our point of views to executive management teams in other functions - HR, Finance etc.

	Total	UK	Germany
Strongly agree	19.5%	25%	14%
Agree	64%	63%	65%
Disagree	13.5%	11%	16%
Strongly disagree	2%	0%	4%
Don't know	1%	1%	1%

IT security leaders appear to be keenly aware of the need for better communication and education about cyber security among their colleagues in other departments across the organization.

80%

agreed or strongly agreed that other departments could have a better understanding of what the security team is trying to accomplish.

83.5%

agreed or strongly agreed that it should be easier to communicate the cyber security perspective to other executives.

Recommendations

While most companies have implemented IT policies around cyber security, they frequently fail to educate employees and clearly communicate to employees the critical nature of their roles and responsibilities. CISOs and IT security leaders need to continually promote the positive effects and value of cyber security to every employee, citing examples and reinforcing the rewards of cyber hygiene at every opportunity. As social engineering threats targeting employees continue to escalate and get more sophisticated, IT security leaders must move beyond negative stereotypes by communicating and motivating managers and employees with more positive messages that demonstrate value in the workplace.

Summary

The CISO needs to be a force for change, whereby perceptions of cyber security among executives and employees are transformed from being simply a security enforcer to that of a business enabler. The CISO will need to become an active member of the executive board, effectively communicating the business case, with metrics that help demonstrate how cyber security reduces risks for the entire organization. Thus, IT security leaders and CISOs should look to prioritizing cyber security solutions that will create a positive experience for employees, emphasizing how they can be more productive and safer when performing their duties.

Free Resources

Privileged Account Management for Dummies eBook

thycotic.com/PAMforDummies

Free eBook written for IT and systems administrators, along with security professionals responsible for protecting their organizations from security threats. It assumes a basic level of IT expertise and experience but is also great for educating business users and board members on the importance of privileged account security practices.

Cybersecurity for Dummies eBook

thycotic.com/
cybesecurityfordummies

Provides a fast, easy read that describes what everyone needs to know to defend themselves and their organizations against cyber attacks —including simple steps everyone can take to protect themselves at work and at home. It empowers your employees to understand, recognize and act on the most common cyber security threats they face in their daily work and personal lives.

About the Survey

Commissioned by Thycotic, the independent market research company Vanson Bourne interviewed 200 IT security decision-makers in November 2018 on the position and reputation of IT security departments in their companies. The sample was comprised of 100 respondents in Germany and 100 in the UK, with 1,000 employees or more from a range of private and public sectors. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About Thycotic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia.

For more information, please visit www.thycotic.com

thycotic