Does someone else own your company's reputation?

EY Global Information Security Survey 2018

Perspectives for technology, media and entertainment, and telco companies

The better the question. The better the answer.
The better the world works.

Building a better
working world

Risking cyber reputations

Are TMT companies doing what's necessary to protect their brands?

The brand – a company's bond with its customers – can take generations to build. Yet the escalating threat of cyber attacks presents the very real possibility of a brand being destroyed overnight.

Given this level of global threat, are technology, media and entertainment, and telco (TMT) companies doing what is necessary to secure their operations, manage cyber risk, protect their customers and safeguard their brands?

In September to November 2017, EY conducted its annual ***Global Information Security Survey*** (GISS) of more than 1,100 executives on key issues in cybersecurity. The global survey panel was drawn from more than 60 countries and represented 20 industries. The following analysis focuses on consolidated findings from TMT companies.

The cyber threat to TMT companies

TMT companies know the value of their brands and their relationships with customers.

Many of these companies are considered leaders in providing product design, customer support and the most attractive customer experience. It is no wonder that 50% of the 10 most admired companies are from the TMT space[1] — far more than any other sector.

But the case can also be made that the TMT sector is more vulnerable to cyber attacks than other industries and that the consequences of a breach are more serious. Consider these issues:

- Many TMT companies are leaders in digital transformation. While digitization may make them more agile and streamline operations, it also increases the number of global attack vectors for cyber attackers. It also exposes virtually every part of their content and operations – from digital rights to trade secrets to semiconductor design to intrusion.
- Traditional industries such as manufacturing and transportation can involve significant switching costs to customers. Not so for many companies in the TMT sector — in which competitors are just a click away for the dissatisfied customer.
- Many TMT companies — particularly those in the technology sector — are held to be the guardians of digital and product security. This sets a higher standard for their security measures — and greater consequences should they fail.
- TMT companies, like many others, are facing a talent shortage in digital transformation, and an especially acute shortage in cybersecurity skills. This leaves them highly exposed to their cyber adversaries.

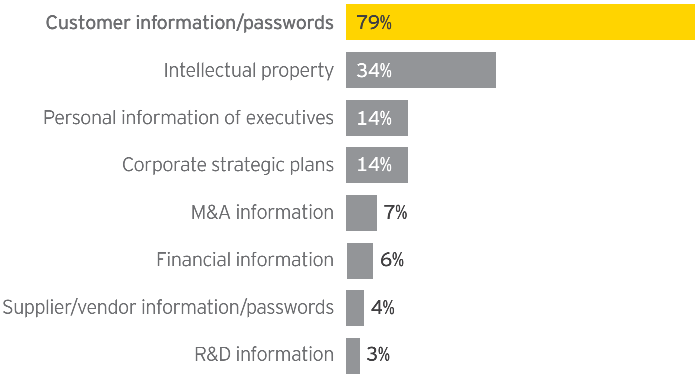
Many TMT companies are leaders in digital transformation.

[1] The World's Most Admired Companies for 2017, Fortune magazine, January 2018, fortune.com/worlds-most-admired-companies/

The cyber threat
to the brand

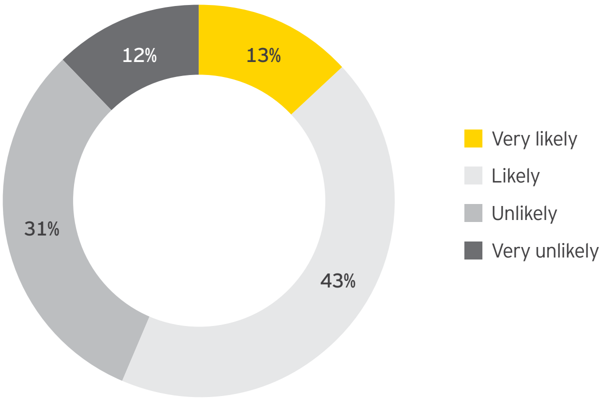
TMT companies recognize the danger that cyber criminals pose to their customer relationships. When asked to identify what proprietary information is most valuable to cyber criminals, TMT companies overwhelmingly identified customer information.

Figure 1: What information in your organization do you consider is the most valuable to cyber criminals? (Select five)



Customer data remains the No. 1 target of the cyber criminal. In a worst-case scenario, a severe breach could create a public perception of a company as an unsafe enterprise to do business with — a negative branding that could take years to recover from and potentially impact its existence.

Figure 2: In your opinion, what is the likelihood of your organization being able to detect a sophisticated cyber attack?



Furthermore, few TMT companies have high confidence that they will be able to detect breaches of their systems, and that they will be able to determine whether customer and other data has in fact been compromised.

Customer data remains the No. 1 target of the cyber criminal.

Committing to protecting the cyber reputation of TMT companies

Given the dangers, one might assume that companies are making cybersecurity a high corporate priority.

But the numbers show otherwise – while global companies spent almost $600 billion on building their brands in 2016,[2] they allocated only about one-tenth of that amount to cybersecurity.[3]

Our research shows that the TMT sector is not an exception. While increasing its absolute cybersecurity spend, the sector is not making anywhere near the commitment that it believes is necessary to safeguard customer data and their brand.

Figure 3: Commitment to cybersecurity by TMT companies

10.6%

Projected growth in cybersecurity budget (next 12 months)

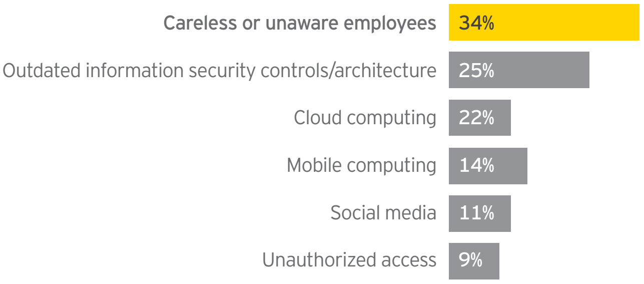
22.2%

Growth in funding needed to protect company in line with company's risk tolerance

In summary, TMT executives believe that their companies are spending less than half of what is necessary to reach acceptable levels of security – creating consequences for their reputations and customer franchises.

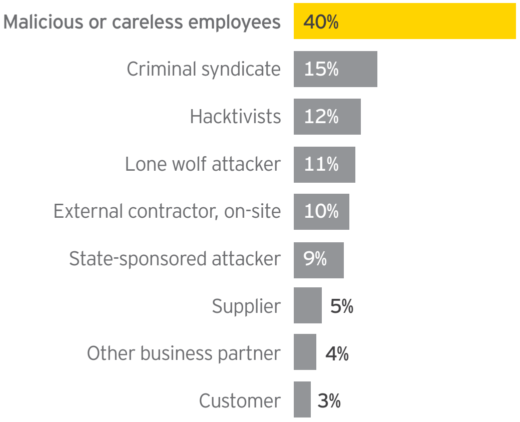
A striking example of this shortfall is in the lack of resources committed to employee awareness and training. We asked TMT executives to assess their companies' cyber vulnerabilities and identify the most likely sources of attacks on their companies. In both cases, the most serious vulnerabilities were linked to employee behavior.

Figure 4: Which vulnerabilities have most increased your risk exposure over the last 12 months? (Selected responses)



Similarly, TMT respondents believe that employees – either through lack of awareness or via malicious acts – are the greatest source of an attack.

Figure 5: What do you consider the most likely source of an attack?

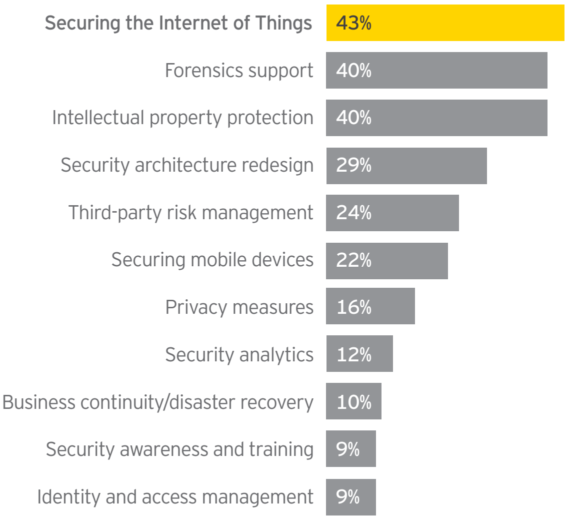


Yet while TMT companies recognize the dangers presented by employees, they place a surprisingly low priority on the training and supervision that are designed to reduce employee-driven cyber risk.

[2] "Global Advertising Spend to Rise 4.6% to $579 Billion in 2016," Zenith Optimedia, cited in Variety, 2016. "Global PR Industry Hits $14bn In 2016 As Growth Slows To 5%," Holmes Report, 2016.

[3] "Cyber security spend $73.7 billion," IDC Worldwide Semiannual Security Spending Guide, 2016.

Figure 6: Which of the following information security areas would you define as high priority for your organization over the coming 12 months? (Select top three)



TMT companies are placing an especially high priority on securing the Internet of Things (IoT). While the IoT has many benefits for TMT companies – digitizing a telco's entire network, or full robotic automation of a semiconductor lab – it can also present higher cyber risk. By placing a company's critical operations on an IoT platform, it can increase the level of vulnerability (e.g., more attack vectors) and present higher consequences of a breach (e.g., ransomware attacks on production systems).

In summary, TMT companies – while acknowledging the risk posed by their employees – are not placing a high enough priority on the means to reduce this risk. This is an important example of an under commitment being made by companies to reach their own standards of cybersecurity.

TMT companies are placing an especially high priority on securing the Internet of Things.

What technology, media and entertainment, and telco companies must do

There is a global consensus that cyber attacks will not only continue but increase in velocity and sophistication, including targeting data, cloud providers, automation and IoT products. Accepting that the brand — the company's bond with its customers — is a critical asset that demands the highest protection, these are a few of the key steps that TMT companies must take:

1. **Place a priority on protection level of brand-related assets:** An emerging view in cybersecurity is that, due to resource constraints, all assets cannot be protected with equal levels of security.
2. **TMT companies should place such a priority on protecting brand-related assets:** Building a "ring fence" around purchasing information, passwords, transaction records, personally identifiable information and other data that touches the customer. This is the information that is most likely to be targeted by cyber attackers, and the breach that can cause the greatest harm to the enterprise – it should be the priority. In addition, TMT companies that build and sell IoT products should manage cybersecurity risks throughout the IoT ecosystem from development, production and most importantly, active maintenance.
3. **Build an employee culture of cybersecurity:** Many cybersecurity programs – managed by IT specialists – focus on highly technical solutions to defend against cyber attacks. Companies should recognize that attackers can potentially be their own employees, and detecting malicious lateral movements inside the network perimeter is equally as important. Cybersecurity training, supervision and accountability – in short, an employee culture of cybersecurity focused on vigilance – are critical to defend against cyber attacks.
4. **Create a post-breach, brand-recovery program:** Many cyber experts privately acknowledge that their companies will be breached at some point. Ability to respond is as important as the capability to defend: companies should have in place a proactive incident response and recovery plan – including a communications plan, incident response process, forensics capability, governance and technical recovery procedures – that can help minimize damage, enable legal diligence and accelerate the company back to the trust of its customers.

For the findings and demographics of the cross-industry EY *Global Information Security Survey*, visit **ey.com/giss.**

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com

About EY Global Technology, Media & Entertainment and Telco services
Digital technology innovation is continuously disrupting organizations and converging industries, driving content distributors into content production, transforming telco providers into content distributors and turning tech companies in all directions. Thus, competition is escalating, and digitally empowered customers are demanding more than ever.

Our global Technology, Media & Entertainment and Telco (TMT) services can help you revamp your organization for the future and enhance customer experiences across all channels. Our network of more than 38,000 TMT professionals helps you nurture growth by bolstering agility, operational excellence and enterprise trust. Our broad advisory, assurance, tax and transaction services help you thrive in this rapidly changing environment — while preparing for disruptions yet to come. Find out more at **ey.com/tmt**

EYG no. 02065-184GBL
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts:

Dave Padmos
EY Global Technology Sector Advisory Leader
+1 206 348 7043
dave.padmos@ey.com

Rob Belk
West Region Cybersecurity Lead
Ernst & Young LLP
+1 858 535 7707
rob.belk@ey.com

Burgess Cooper
Cybersecurity Advisory Services Lead
Ernst & Young LLP
+91 993 081 8333
burgess.cooper@in.ey.com

M.J. Vaidya
Cybersecurity Advisory Services Lead
Ernst & Young LLP
+1 404 541 7039
mj.vaidya@ey.com