

**CYBERSECURITY: THE
INSIGHTS YOU NEED FROM
HARVARD BUSINESS
REVIEW**

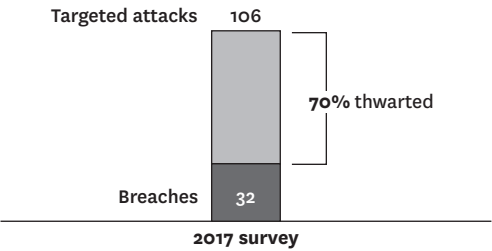
**BY ALEX BLAU, ANDREW BURT,
BORIS GROYSBERG, &
HARVARD BUSINESS REVIEW**

Contents

Figure 2-1: Average annual number of targeted attacks and breaches per company.	3
Figure 2-2: Even though we're thwarting more attacks, we're not preventing more breaches.	4
Figure 2-3: Average cost of cybercrime per company (US\$M)	5
Figure 2-4: Attacks come mostly from outsiders	6
Figure 2-5: Attacks still fail more often than they succeed	7
Figure 2-6: Personal information and payment information are the most commonly compromised targets	8
Figure 2-7: What hackers attack most often, and what they attack most successfully, aren't always the same	9
Figure 2-8: Average cost of cybercrime per company in selected countries (US\$M)	10
Figure 2-9: Average annualized cost of cybercrime by sector, worldwide (US\$M)	11
Figure 2-10: Share of costs per type of activity	12
Figure 2-11: Share of costs per consequence of attack	13
Figure 3-1: Most board directors aren't highly concerned about or ready for cyberthreats	14
Figure 3-2: Few board directors view cybersecurity as a strategic threat	15
Figure 3-3: Most board cybersecurity processes fall short, according to directors	16
Figure 3-4: Cybersecurity is the biggest challenge for board directors	17

FIGURE 2-1

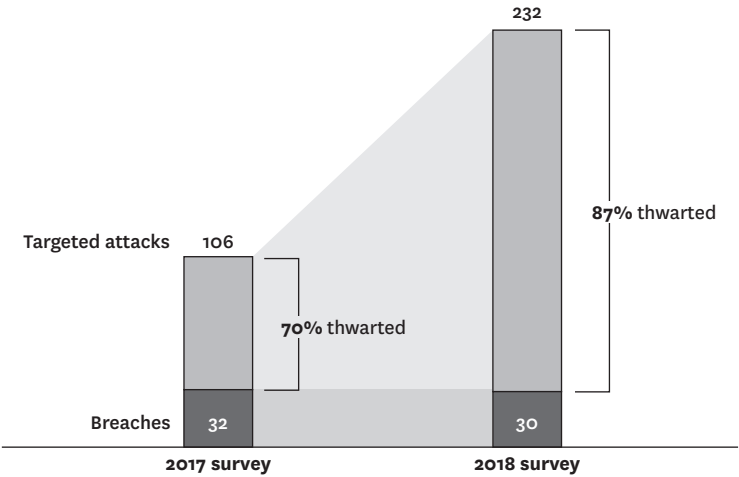
Average annual number of targeted attacks and breaches per company



Source: Accenture, “2018 State of Cyber Resilience: Gaining Ground on the Cyber Attacker”

FIGURE 2-2

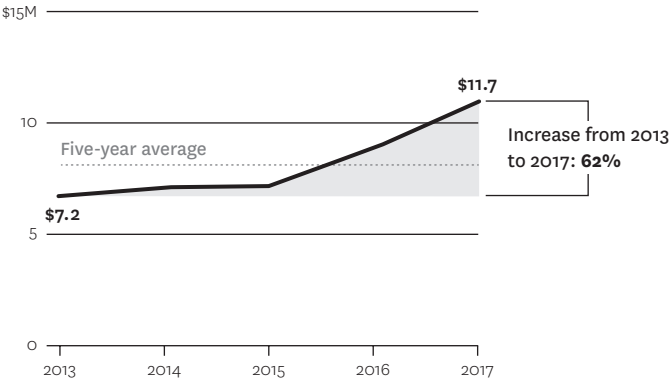
Even though we’re thwarting more attacks, we’re not preventing more breaches



Source: Accenture, “2018 State of Cyber Resilience: Gaining Ground on the Cyber Attacker”

FIGURE 2-3

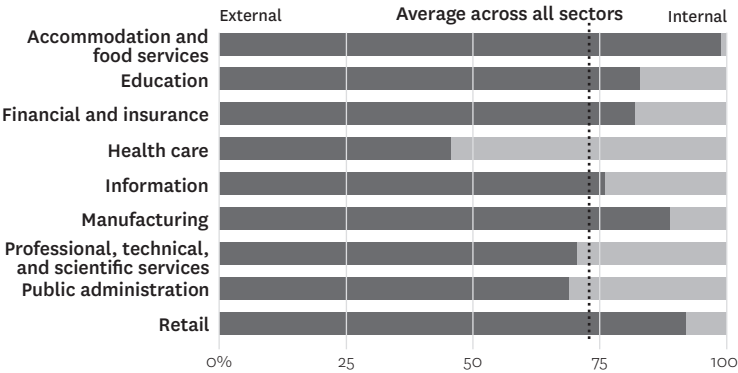
Average cost of cybercrime per company (US\$M)



Source: Accenture and Ponemon Institute, “2017 Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference”

FIGURE 2-4

Attacks come mostly from outsiders

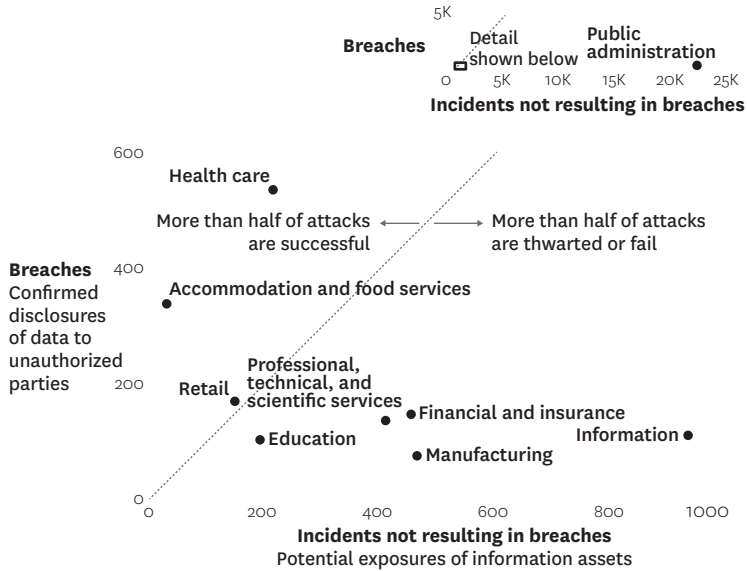


Note: Some external totals include partners and/or multiple parties.

Source: Accenture, “2018 Data Breach Investigations Report”

FIGURE 2-5

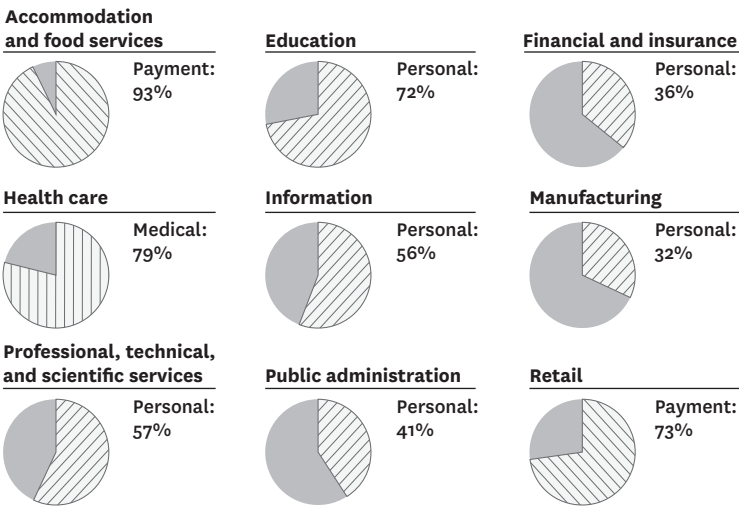
Attacks still fail more often than they succeed



Source: Verizon, "2018 Data Breach Investigations Report"

FIGURE 2-6

Personal information and payment information are the most commonly compromised targets



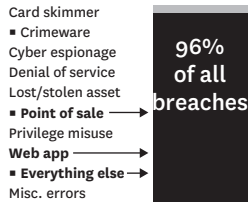
Source: Verizon, “2018 Data Breach Investigations Report”

FIGURE 2-7

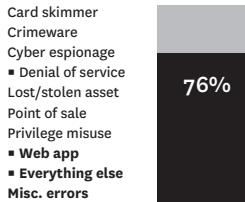
What hackers attack most often, and what they attack most successfully, aren't always the same

Major sources of breaches are in bold and black; major sources of incidents are (■) bulleted.

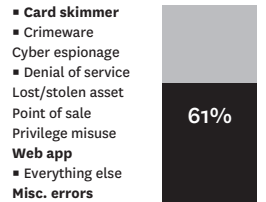
Accommodation and food services



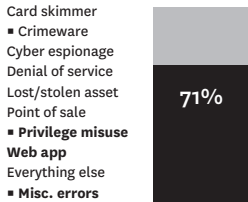
Education



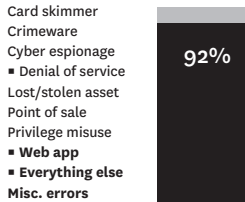
Financial and insurance



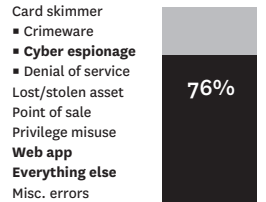
Health care



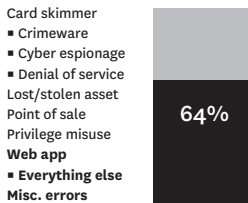
Information



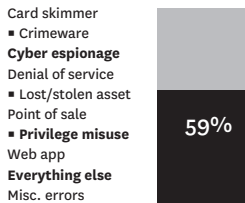
Manufacturing



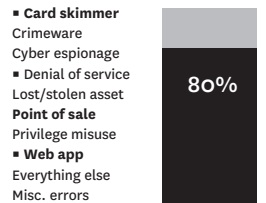
Professional, technical, and scientific services



Public administration



Retail



Note: Professional, technical, and scientific services has four bulleted items because of a tie.

Source: Verizon, "2018 Data Breach Investigations Report"

FIGURE 2-8

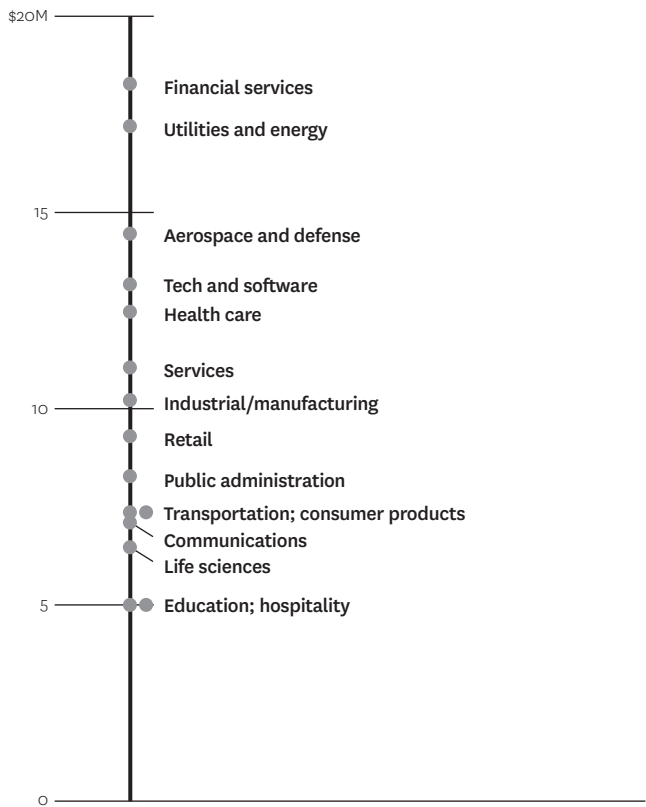
Average cost of cybercrime per company in selected countries (US\$M)



Source: Accenture and Ponemon Institute, “2017 Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference”

FIGURE 2-9

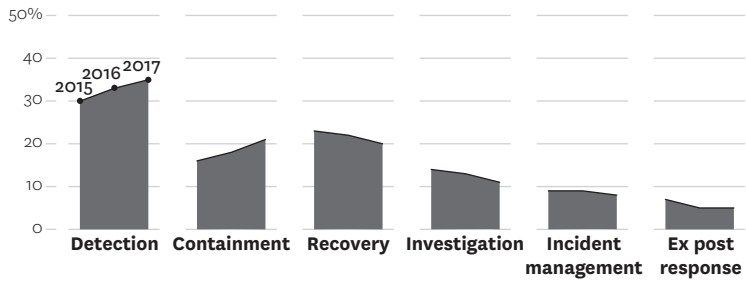
Average annualized cost of cybercrime by sector, worldwide (US\$M)



Source: Accenture and Ponemon Institute, “2017 Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference”

FIGURE 2-10

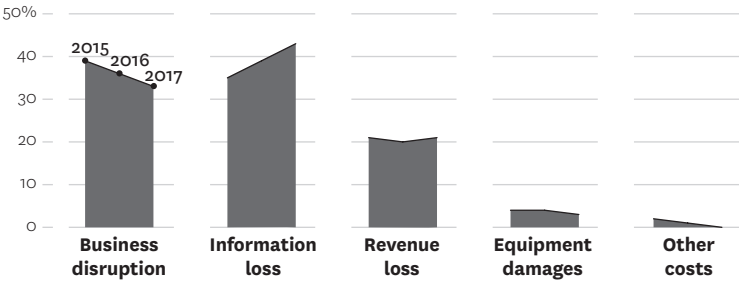
Share of costs per type of activity



Source: Accenture and Ponemon Institute, "2017 Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference"

FIGURE 2-11

Share of costs per consequence of attack

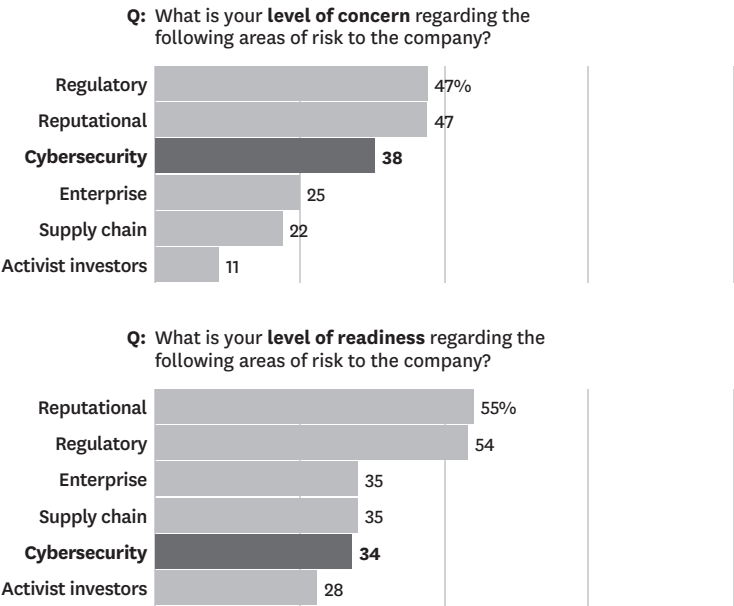


Source: Accenture and Ponemon Institute, “2017 Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference”

FIGURE 3-1

Most board directors aren't highly concerned about or ready for cyberthreats

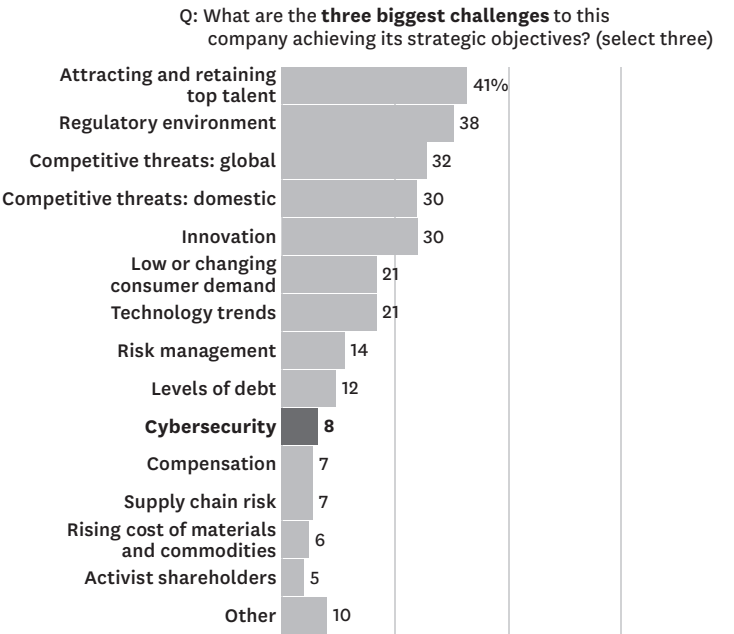
Percentage that indicated a “great” or “very great” level of concern/readiness



Number of participants: 340

FIGURE 3-2

Few board directors view cybersecurity as a strategic threat

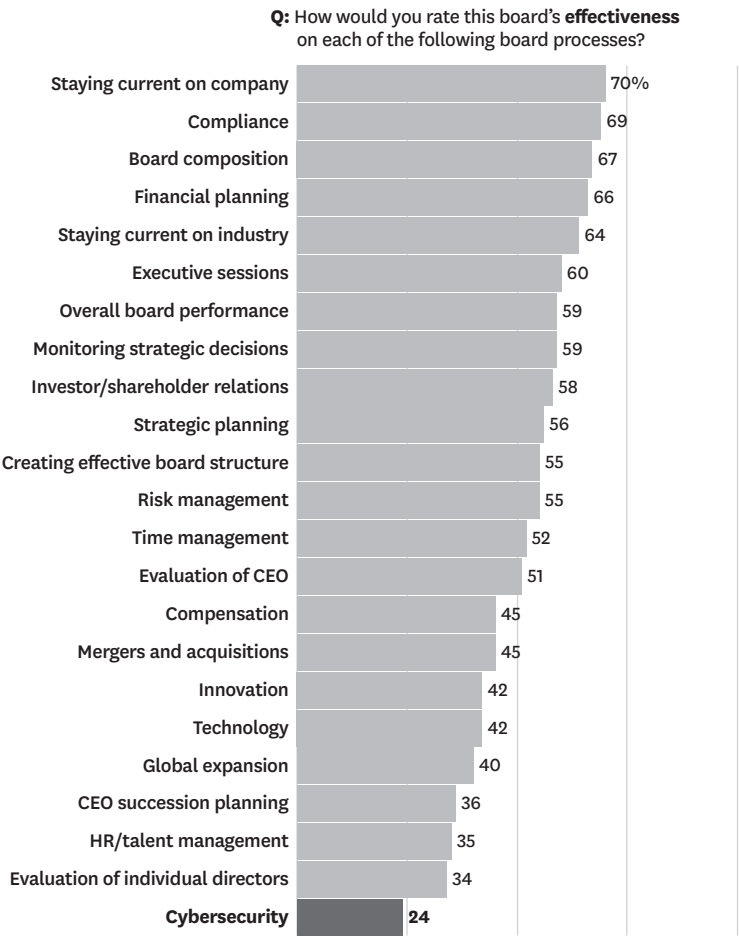


Number polled: 2,938

FIGURE 3-3

Most board cybersecurity processes fall short, according to directors

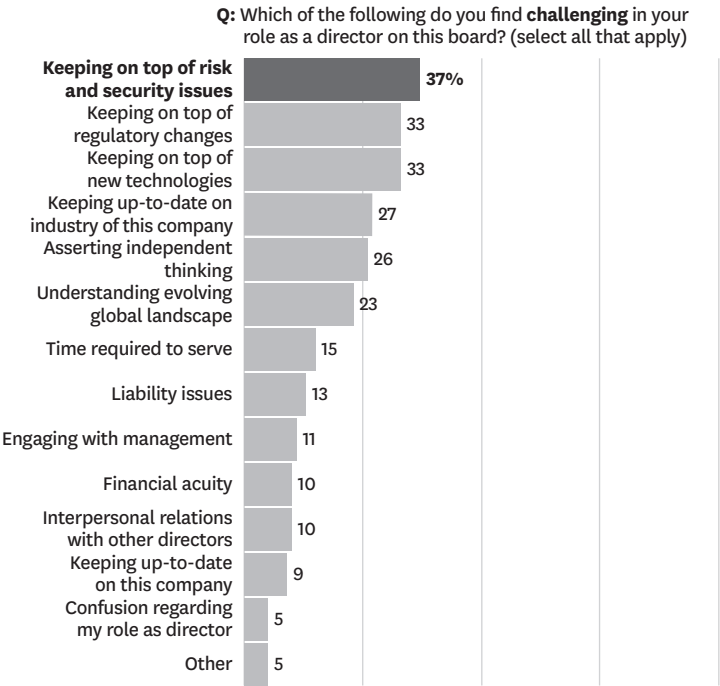
Percentage that rated each process as “above average” or “excellent”



Number of participants: 3,183

FIGURE 3-4

Cybersecurity is the biggest challenge for board directors



Number of participants: 2,791