UNLOCKING THE VALUE OF IMPROVED CYBERSECURITY PROTECTION

NINTH ANNUAL COST OF CYBERCRIME STUDY IN FRANCE

accenturesecurity

THE GLOBAL STORY IN BRIEF

The expanding threat landscape and new business innovation is leading to an increase in cyberattacks.

- The **threat landscape** continues to **expand** with an increase in **nation-state espionage**, **supply chain** and **critical infrastructure** threats.
- In the drive for growth and innovation, **79%** of business leaders say **new business models** introduce **technology vulnerabilities** faster than they can be secured.
- The average number of **security breaches** in the last year grew by **11%** from **130** to **145.**

Organizations spend more than ever to deal with the costs and consequences of more sophisticated attacks.

- The average cost of cybercrime for an organization increased US$1.4M to **US$13.0M.**
- **Phishing** and social engineering (+16%), **ransomware** (+15%), and **stolen devices** (+15%)—largely **people-based attacks**—show the biggest increases.
- **Information theft** is the most expensive consequence of cybercrime and companies spend most on **discovery** activities.

What is the economic value of improving cybersecurity protection worth to an organization?

- Improving **cybersecurity protection** can **reduce the cost** of cybercrime and provide **additional revenue** opportunities. A **total** of **$US5.2 trillion** over the next five years.
- This translates into additional revenue of **2.8 percent**—or an average of **$US580M** annually—in each of the next five years for an average G2000 company.
- This provides a **useful benchmark** to measure investments in cybersecurity protection.

Prioritize technologies that reduce the consequences of cybercrime to unlock future economic value.

- Place greater emphasis on **protecting people** to combat the rise in attacks against them.
- Prioritize technologies to **limit information loss and business disruption** which are the **largest consequences** of cybercrime and a growing concern with **new privacy regulation** like GDPR and CCPA.
- Use **automation** (including AI and machine learning) and **advanced analytics** to manage the rising **cost of discovering attacks.** the largest component of spend.

ABOUT THE RESEARCH

EXAMINING THE ECONOMIC IMPACT OF CYBER ATTACKS

9th **Annual research study**

11 Countries

US
United Kingdom
Japan
Germany
France
Brazil
Canada
Australia
Spain
Italy
Singapore

355 Companies

16 Industries

Travel
Comm & Media
Life sciences
Retail
Health
Consumer Goods
Public Sector
US Federal
Energy
Capital Markets
High Tech
Insurance
Automotive
Software
Utilities
Banking

2,647 Interviews

Jointly developed by:

accenture

Ponemon INSTITUTE

DEFINING CYBERATTACKS AND SECURITY BREACHES

What types of cyberattacks and security breaches are included in this research?

We define **cyberattacks** as malicious activity conducted against the organization through the IT infrastructure via the internal or external networks or the Internet. Cyberattacks also include attacks against industrial control systems (ICS).

A **security breach** is one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

WITH AN EXPANDED THREAT LANDSCAPE AND NEW DIGITAL VULNERABILITIES, THE NUMBER OF SECURITY BREACHES INCREASED IN THE LAST YEAR

Average number of security breaches in 2017 in France

69

+14%

Increase in one year

Average number of security breaches in 2018 in France

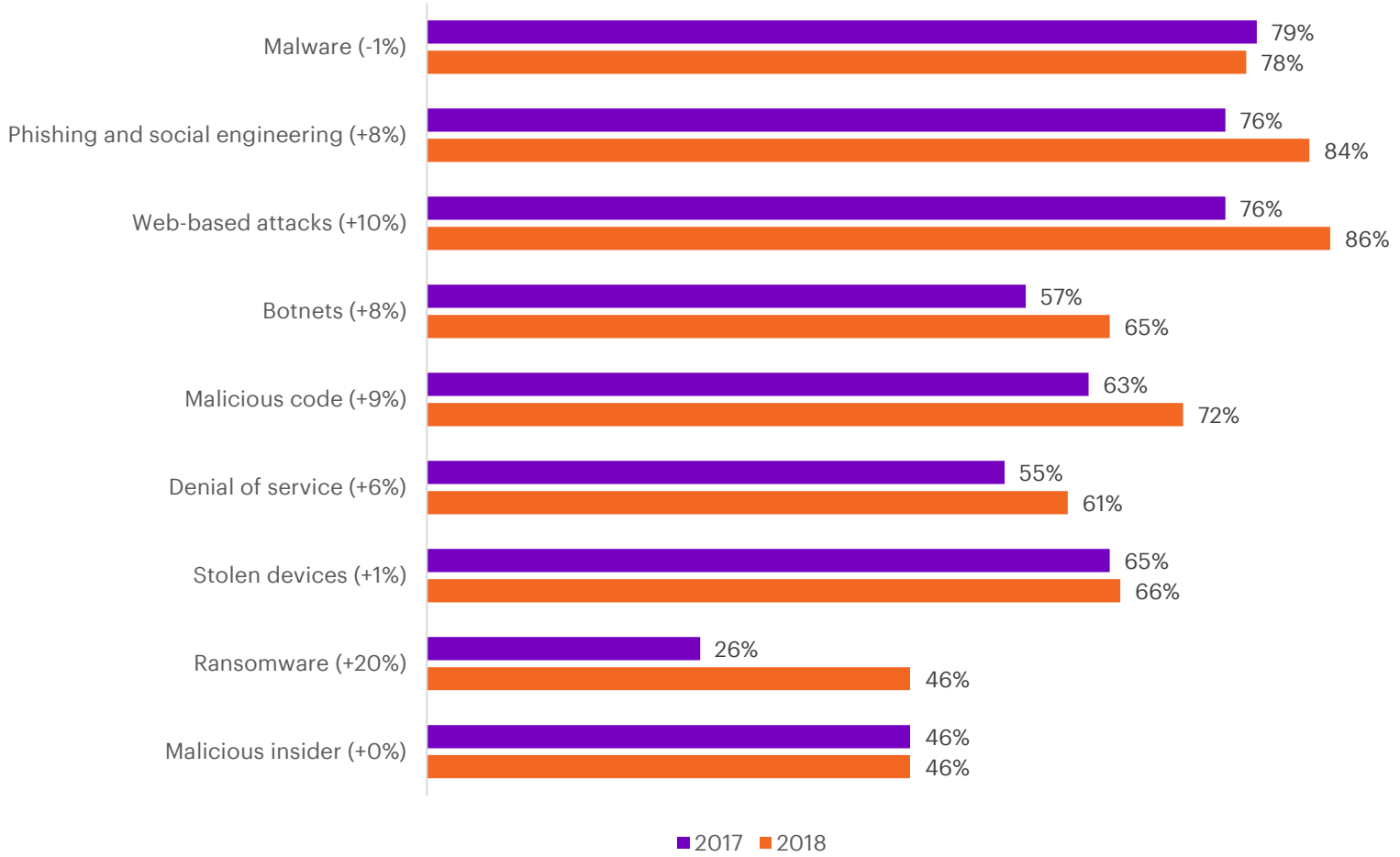
80

*** 31 French companies, 248 interviews**

THE LARGEST INCREASES COME FROM THE NUMBER OF ORGANIZATIONS EXPERIENCING PEOPLE-BASED ATTACKS

Types of cyberattacks experienced by French companies
(% increase 2017–2018)

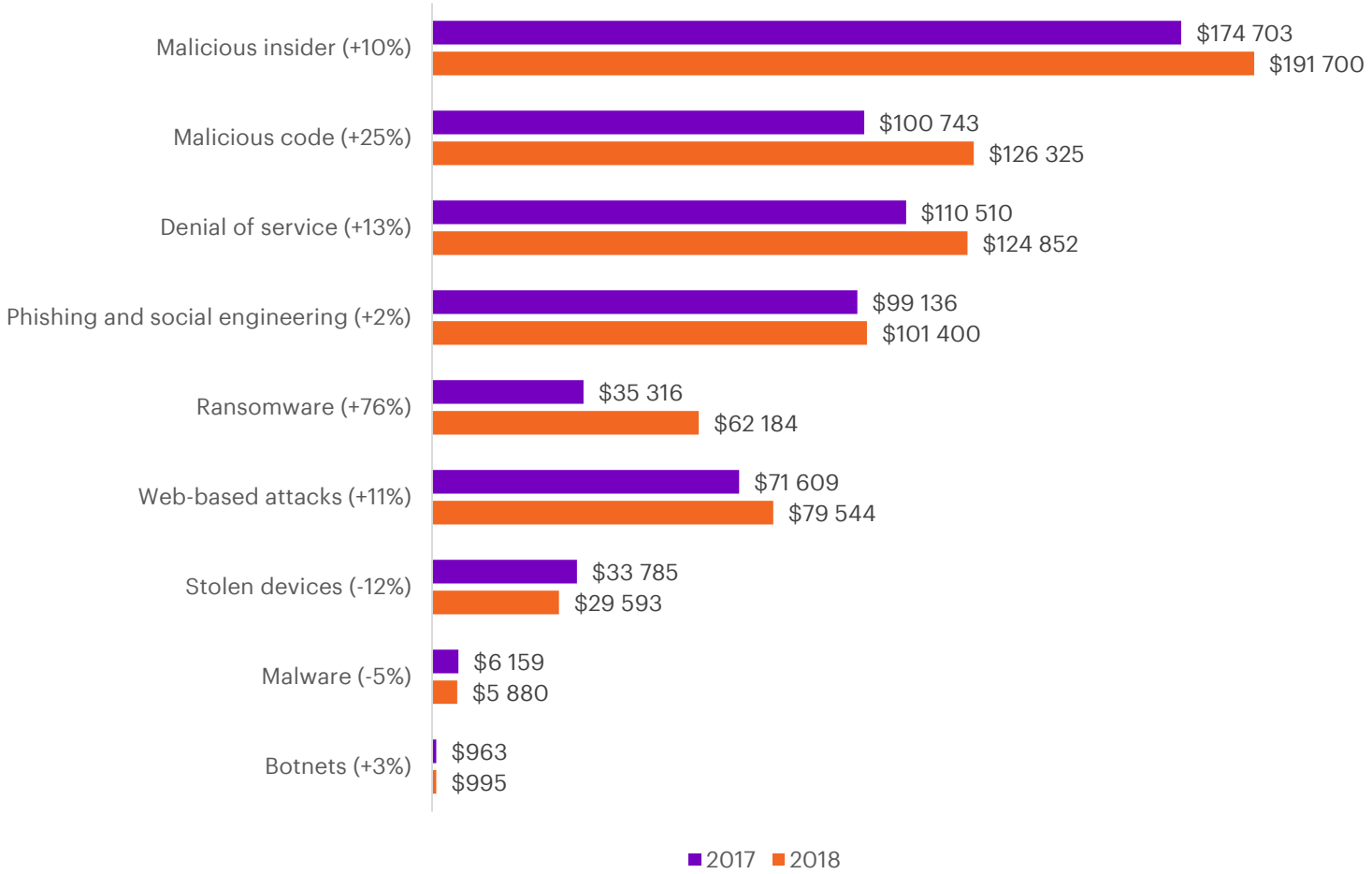
Phishing (+12%) and Ransomware (+20%)



INDIVIDUAL INCIDENTS ARE BECOMING MORE EXPENSIVE TO RESOLVE

Types of cyberattacks experienced by French companies
US$ (% increase 2017–2018)

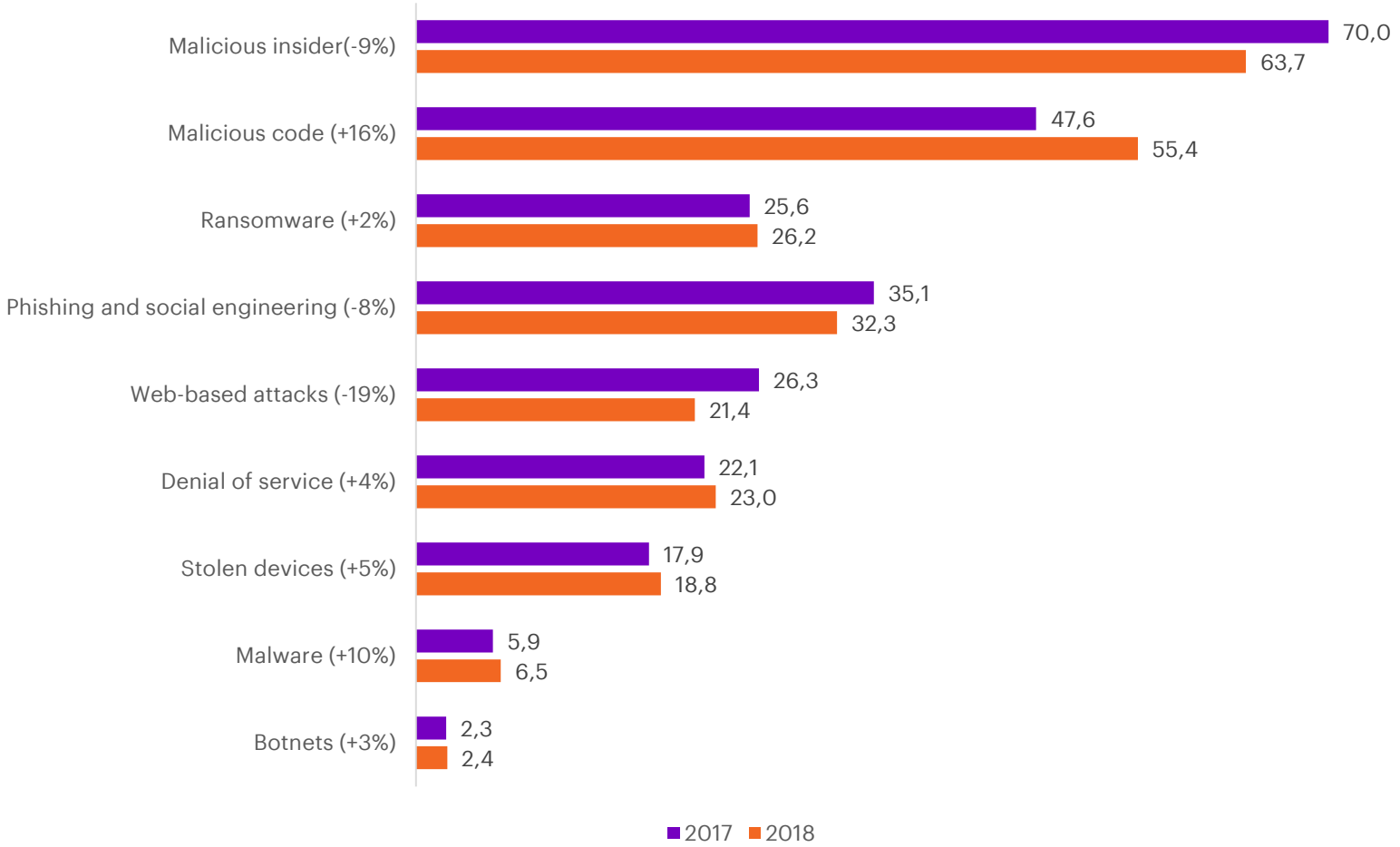
Malicious Insiders increased (+10%), Malicious Code (+25%) and Ransomware an alarming (+76%)



MANY ATTACK TYPES ARE TAKING MORE TIME TO RESOLVE

Length of time taken to resolve cyberattacks for French Companies
Days (% increase 2017–2018)

Malicious code attacks shows the most significant increase in the number of days taken to resolve (+16%).



CALCULATING THE COST OF CYBERCRIME

Organizations were asked to report their **spend** (costs) to **discover, investigate, contain** and **recover** from cyberattacks over four consecutive weeks. Also covered are the expenditures that result in after-the-fact activities and efforts to **reduce business disruption** and the **loss of customers.**

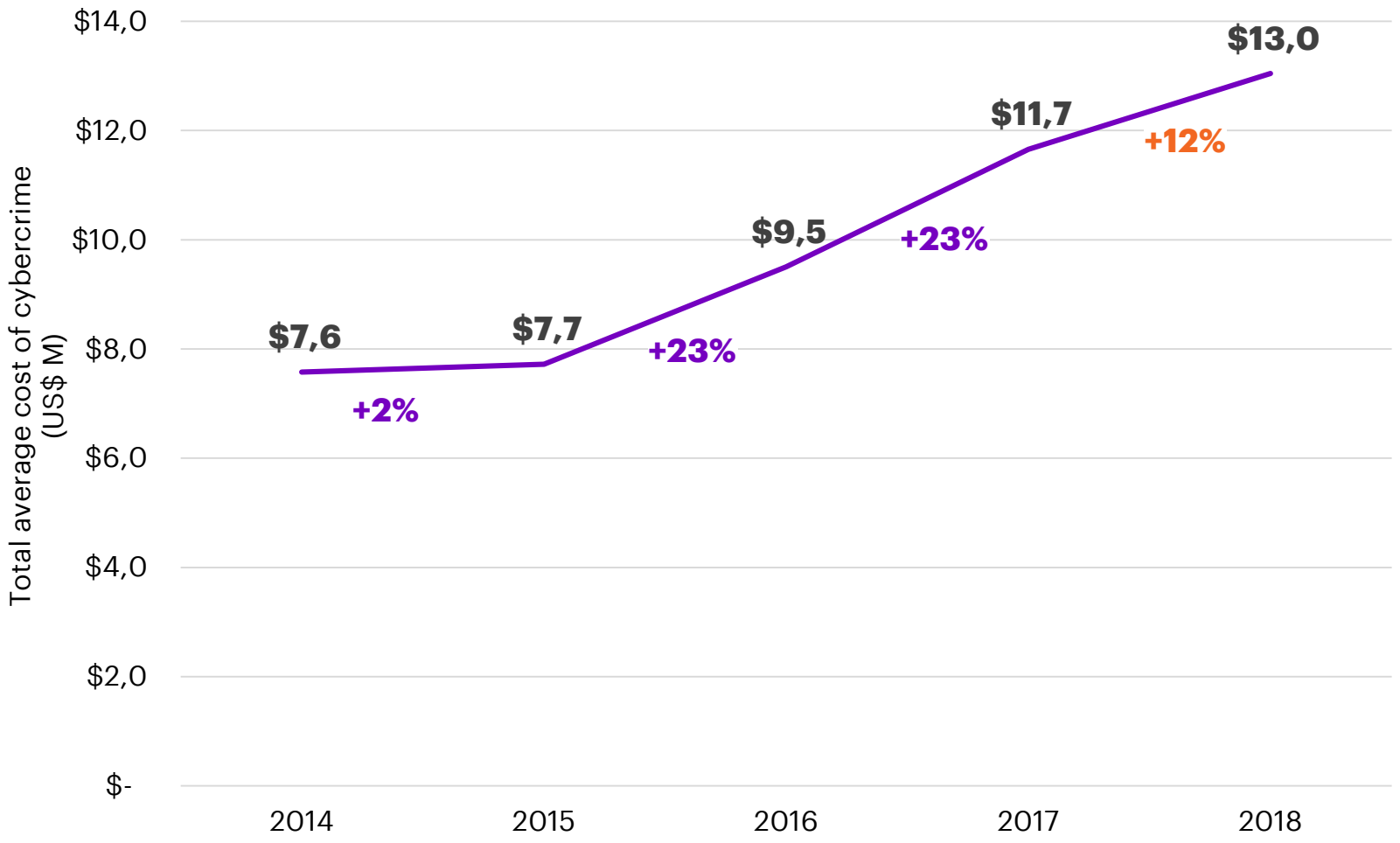
These costs **do not include** outlays and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Once compiled and validated, these costs were then grossed-up to determine the **annualized cost.**

THE AVERAGE COST OF CYBERCRIME FOR AN ORGANIZATION INCREASED BY 12 PERCENT OVER THE YEAR TO US$13.0 MILLION

The GLOBAL average cost of cybercrime for companies in study
US$

The increase over the last five years is 72%, or US$ 5.5 million, on average for companies in our study.

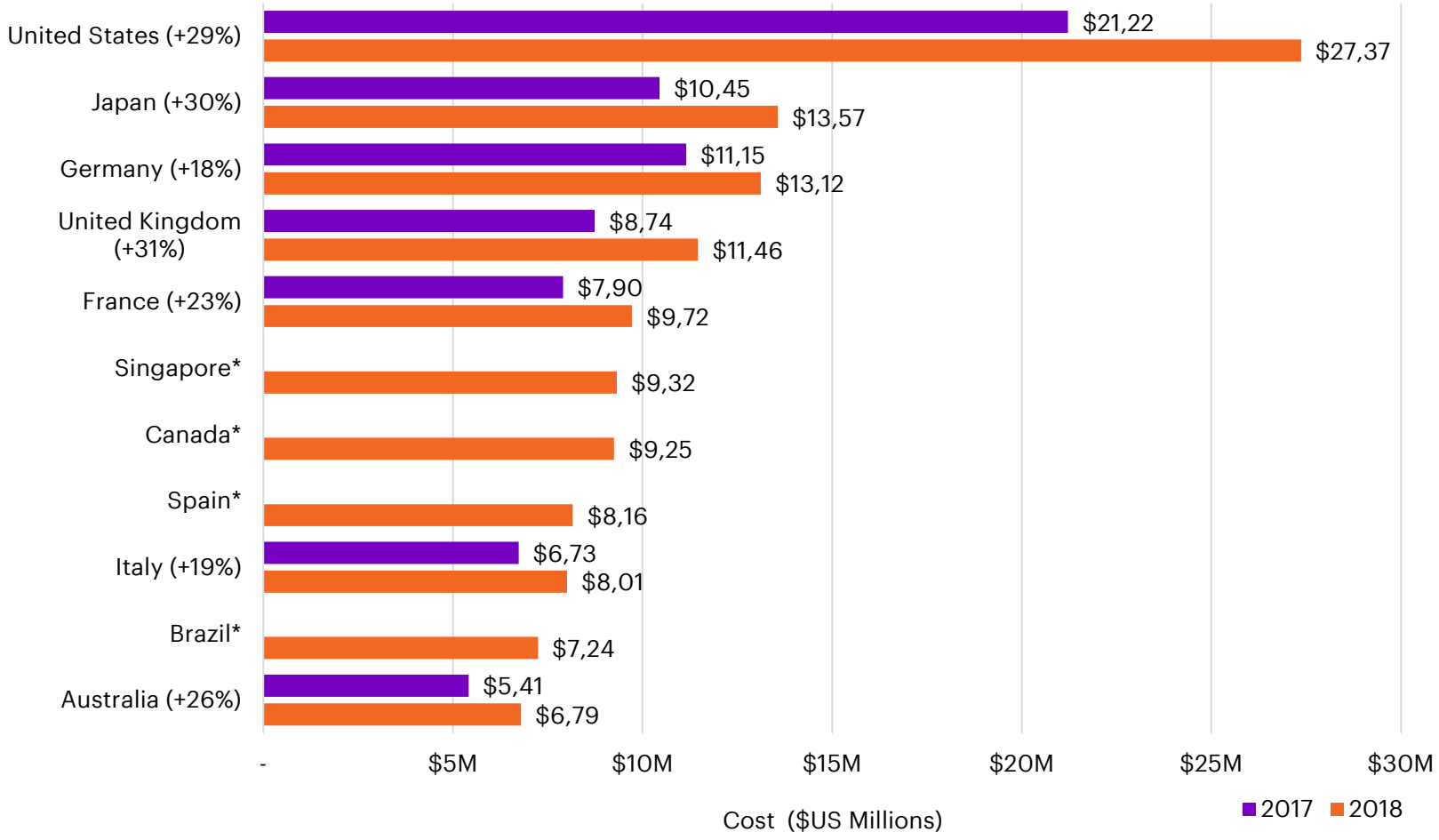


THE COST OF CYBERCRIME IS INCREASING IN ALL COUNTRIES

Change in cybercrime cost by country
US$ millions
(% increase 2017–2018)

The average increase in cybercrime costs for the countries in our sample is +26%. The United Kingdom (31%), Japan (31%) and United States (29%) have the largest increases followed by Australia (+26%).

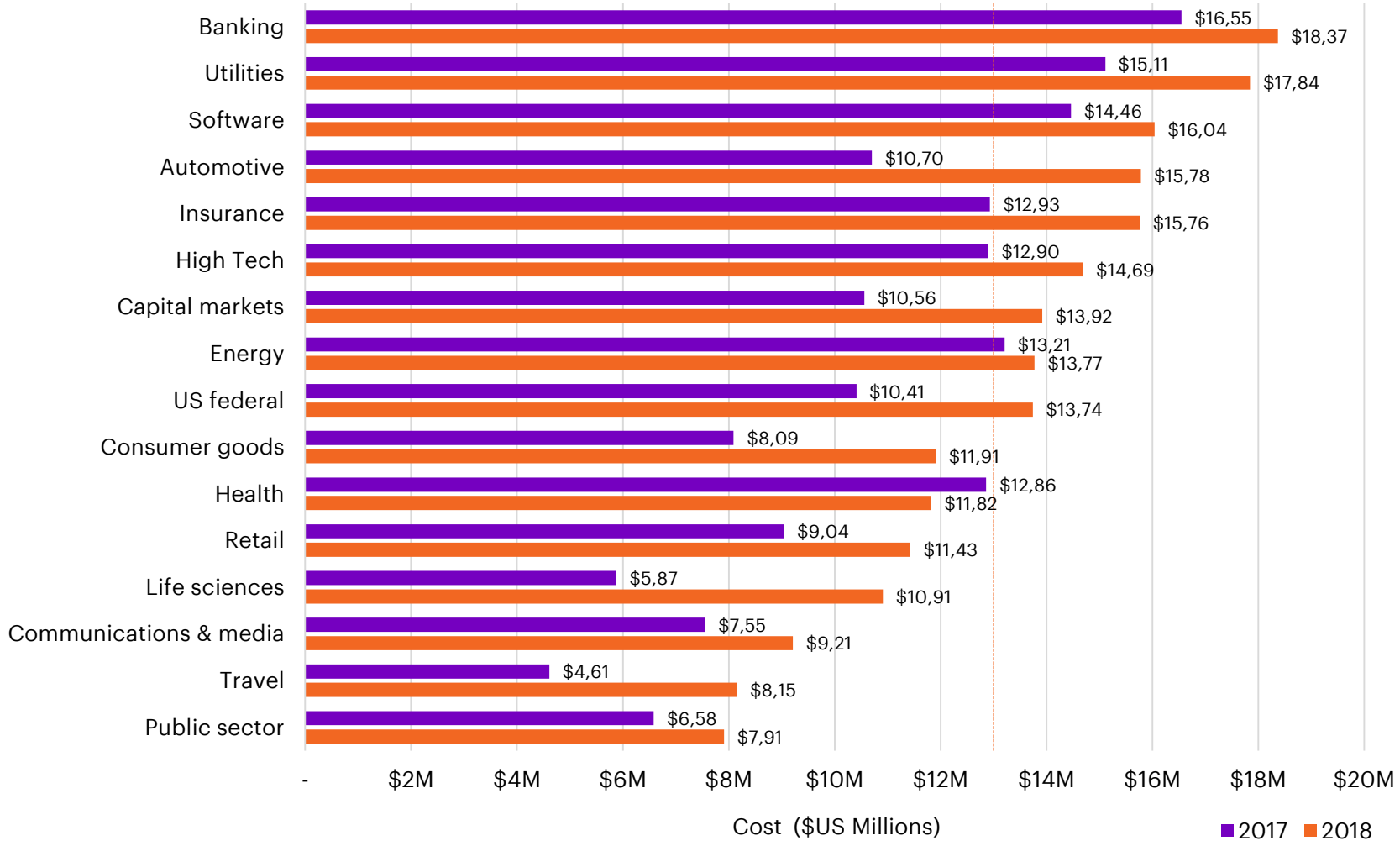
The increase for Germany (18%) is less than half the increase in 2017 (42%).



BANKING AND UTILITIES CONTINUE TO HAVE THE LARGEST COST OF CYBERCRIME BY INDUSTRY

Average annualized cost by industry sector
US$ (million)

Average cost of cybercrime = US$13.0 million



THE VALUE OF CYBERSECURITY

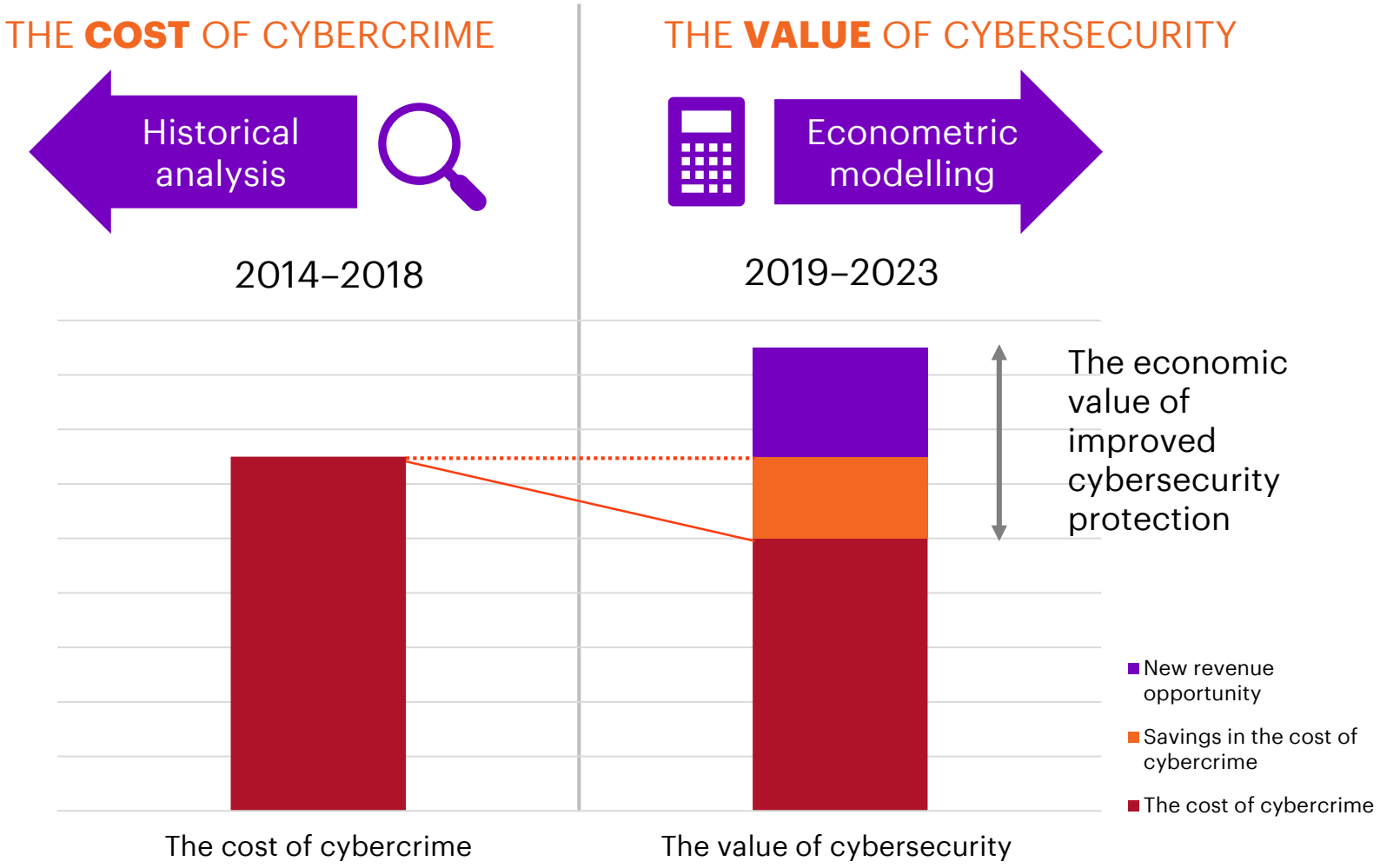
What is the economic value of improving cybersecurity protection worth to an organization?

HOW MUCH IS IMPROVED CYBERSECURITY PROTECTION WORTH TO A BUSINESS?

There is a positive correlation between size and cost. The bigger the organization the bigger the cost burden on them.

But can improved cybersecurity protection create more **economic value** for businesses?

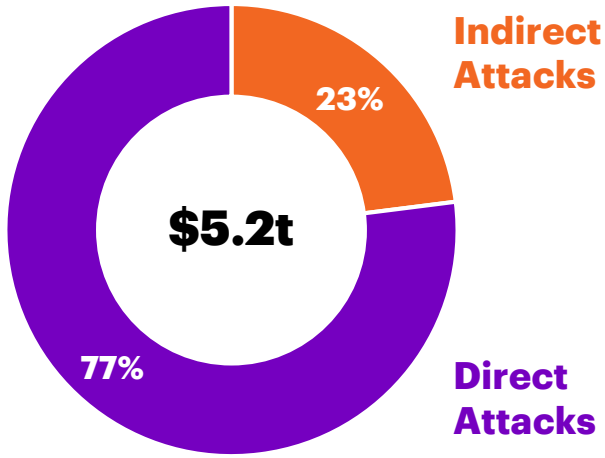
Economic value includes **savings** in the cost of cybercrime plus **new revenue** opportunity.



THE ECONOMIC VALUE AT RISK DUE TO CYBERATTACKS OVER THE NEXT FIVE YEARS IS $5.2 TRILLION GLOBALLY

Value at risk: 2019–2023

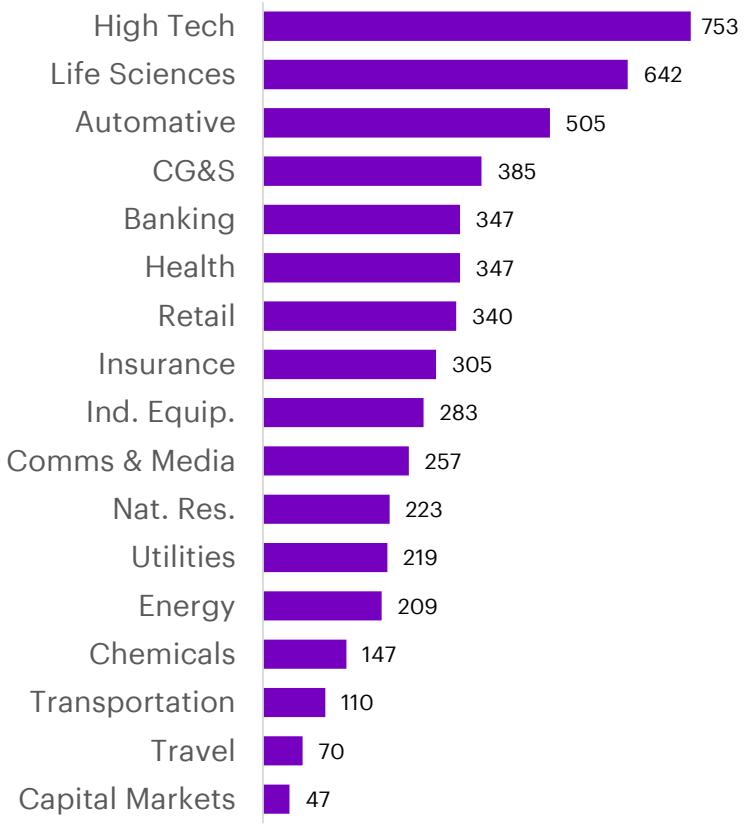
(Value at Risk* due to direct and indirect attacks, Cumulative 2019–2023, US$t)



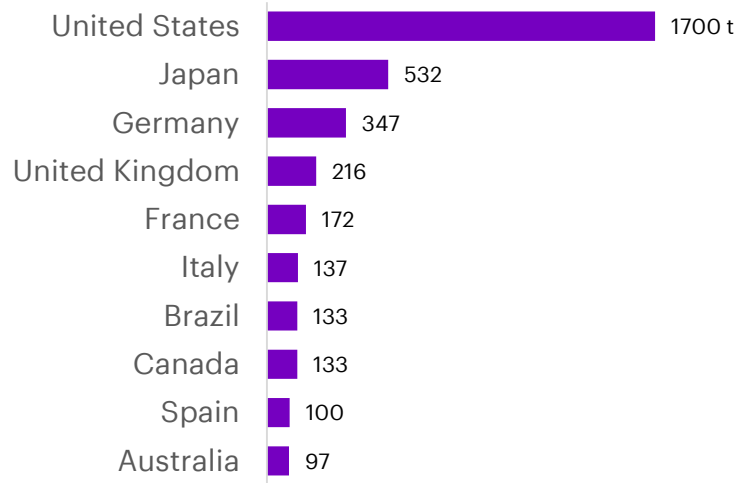
Source: Accenture Research

* Expected loss of savings in cybersecurity spend and revenue opportunity over the next 5 years. Calculations over a sample of 4,700 global public companies.

Value at risk by industry (US$Bn)



Value at risk by country (US$Bn)



THE ECONOMIC VALUE AT RISK PROVIDES A USEFUL BENCHMARK FOR SECURITY INVESTMENTS

Average annualized cost by industry sector
US$ (million)

The average G2000 company revenue in 2018 was US$20 billion.

Life sciences and high tech companies have the highest revenue at risk.

Capital markets and industrial equipment companies have the lowest revenue at risk.

Industry	Revenue at Risk (CAGR 2019 – 2023) Global=2.8%	2018 Average G2000 Revenue (USD$ M)	Average annual revenue opportunity at risk 2019–2023 (US$ M)	2019 –2023 Cumulative revenue opportunity at risk (USD$ M)
Automotive	3.1%	$20,000	$770	$3,851
Banking	2.4%	$20,000	$570	$2,848
CG&S	3.4%	$20,000	$738	$3,689
Capital Markets	1.5%	$20,000	$365	$1,826
Chemicals	2.7%	$20,000	$572	$2,859
Comms & Media	2.0%	$20,000	$456	$2,282
High Tech	4.5%	$20,000	$1,056	$5,278
Energy	2.1%	$20,000	$352	$1,762
Health	3.7%	$20,000	$1,156	$5,779
Industrial Equipment	1.5%	$20,000	$368	$1,841
Insurance	3.9%	$20,000	$949	$4,743
Life Sciences	5.6%	$20,000	$1,475	$7,375
Natural Resources	2.6%	$20,000	$541	$2,703
Retail	1.5%	$20,000	$339	$1,695
Transportation	1.6%	$20,000	$343	$1,715
Travel	1.5%	$20,000	$378	$1,891
Utilities	2.9%	$20,000	$579	$2,895

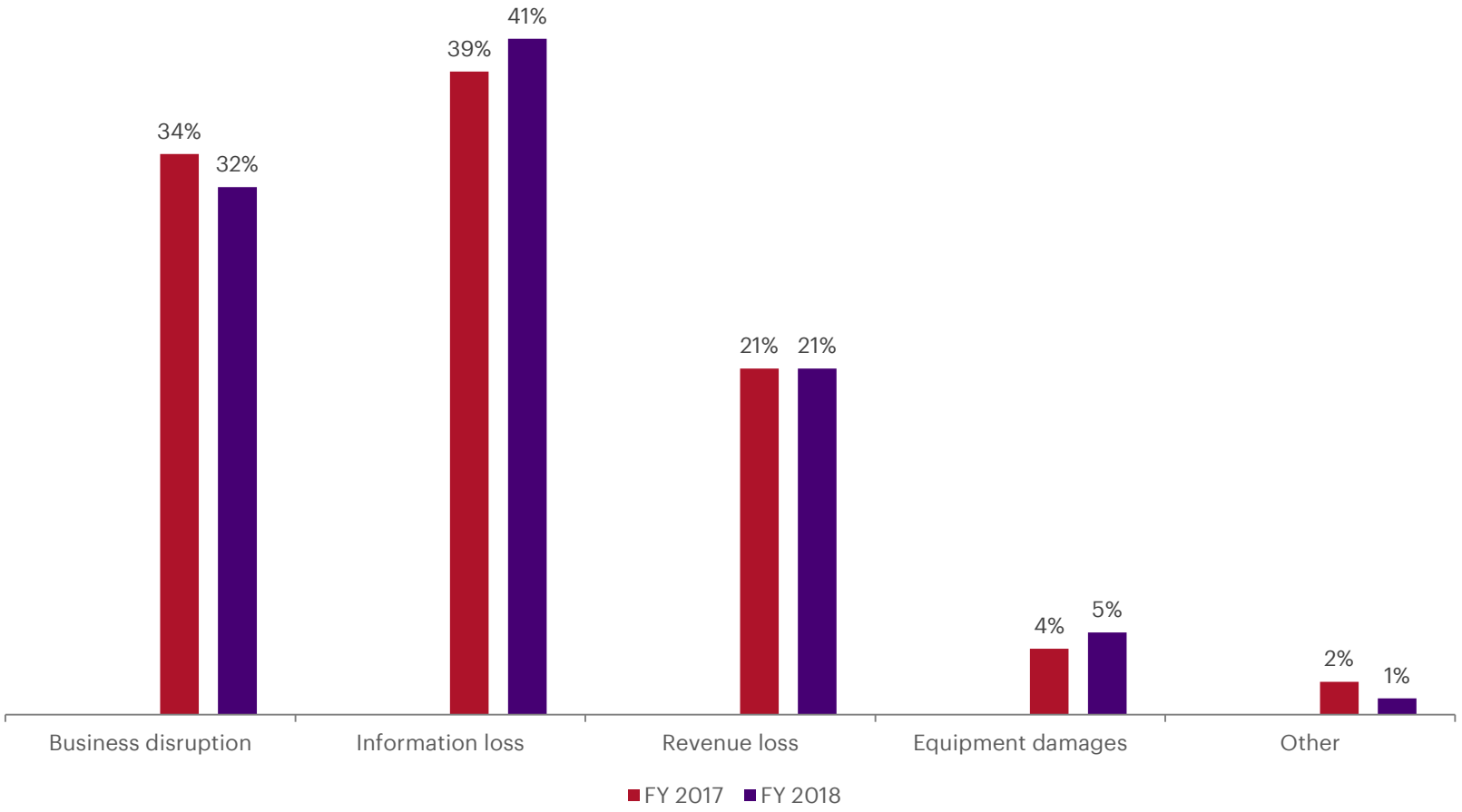
THE VALUE OF CYBERSECURITY

Prioritize technologies that reduce the costs and consequences of cybercrime to unlock future economic value.

INFORMATION LOSS REMAINS THE MOST EXPENSIVE CONSEQUENCE OF A CYBERCRIME

Percentage cost by consequence for French Companies

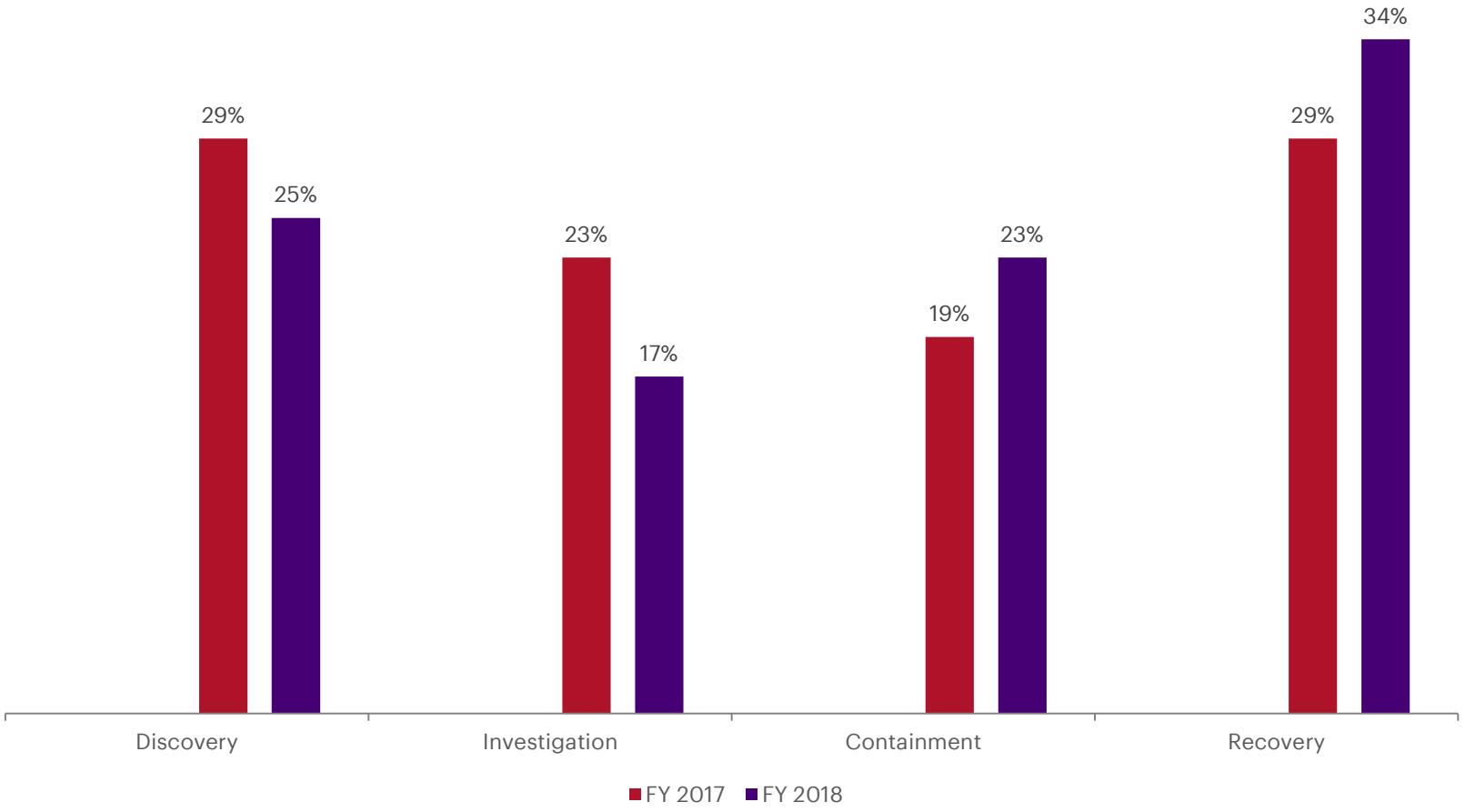
Information loss is a worrying trend with new regulation like GDPR and CCPA to consider.



COMPANIES SPEND THE MOST ON RECOVERY AND THE LEAST ON INVESTIGATION ACTIVITIES

Percentage cost by internal activities for French Companies

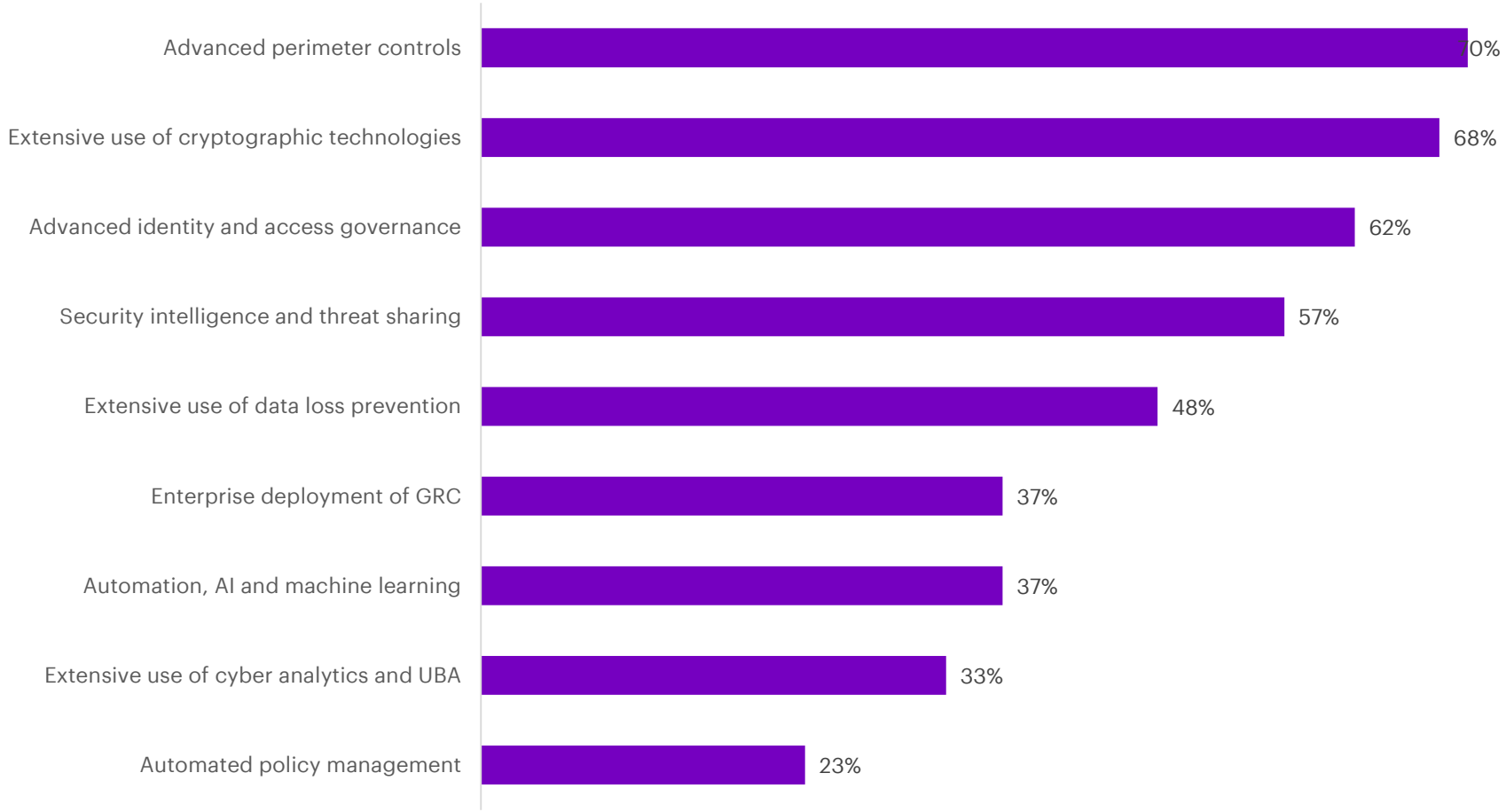
Discovery and recovery spend highlight a significant cost-reduction opportunity for organizations that are able to systematically deploy enabling security technologies to help facilitate the discovery-to-recovery cycle.



PERIMETER CONTROLS ARE FULLY DEPLOYED BY MORE COMPANIES THAN ANY OTHER SECURITY TECHNOLOGY

The proportion of French companies who deploy nine enabling security technologies

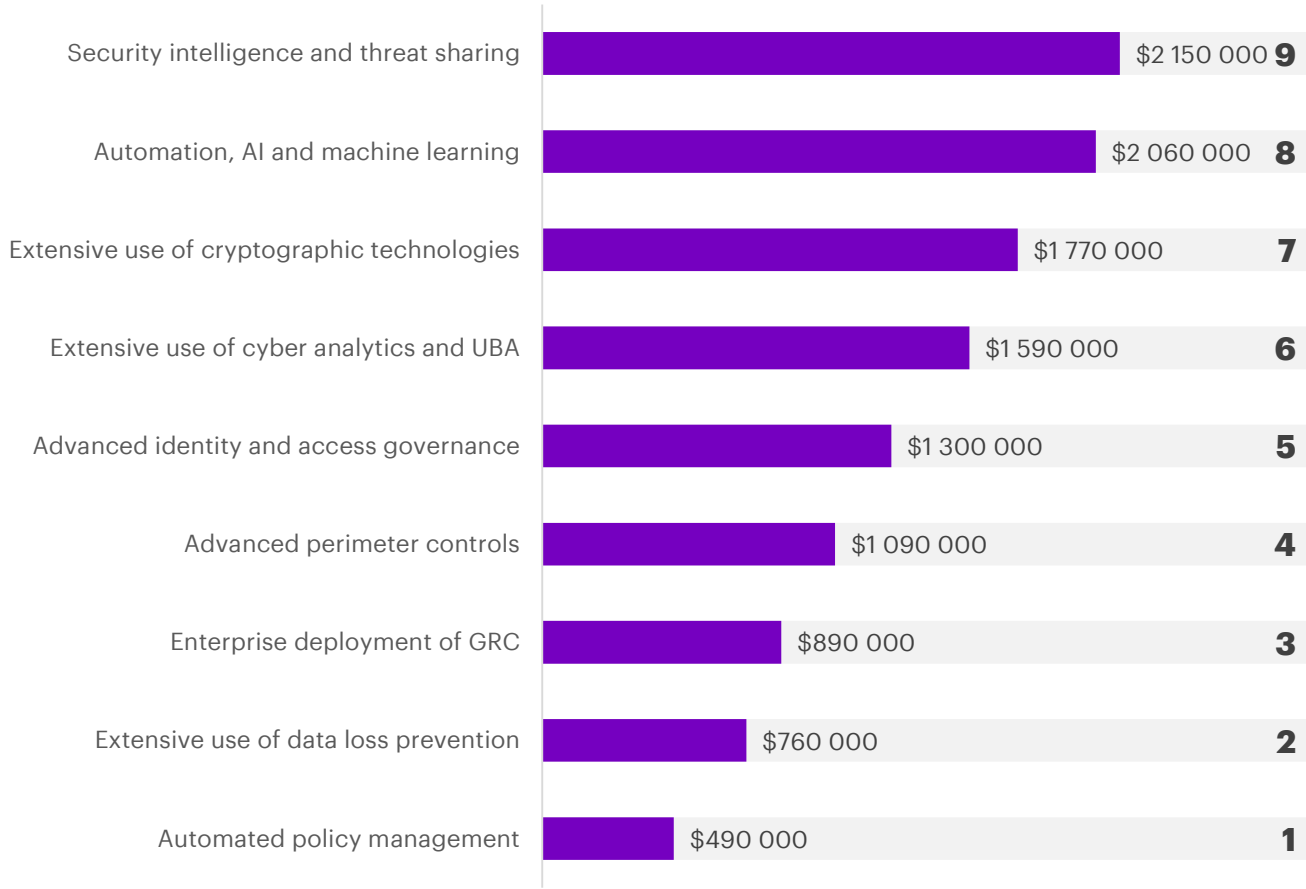
The deployment of Automation, AI and machine learning as well as cyber and user behavior analytics remains stubbornly low.



SECURITY INTELLIGENCE AND THREAT SHARING DELIVER THE LARGEST COST SAVINGS WHEN FULLY DEPLOYED

Cost savings when deploying enabling technologies for French Companies
US$

While not widely used as yet, automation (with AI and machine learning) and extensive use of cyber analytics can provide significant cost savings on average.



PRIORITIZE BREAKTHROUGH INNOVATIONS LIKE AI AUTOMATION AND ANALYTICS

ORGANIZATIONS NEED TO:

1. Place greater emphasis on **protecting people** due to the rise in phishing, ransomware and malicious insider attacks

2. Invest to **prevent information loss and business disruption** which are growing concerns with **new privacy regulation** like GDPR and CCPA.

3. Use **automation** and **advanced analytics** to manage the rising **cost to discover attacks** which is the largest component of spend.

55 days

The time to resolve **denial of service** attacks increased by 16 percent

41% of cost

Information loss remains the most expensive consequence of cybercrime

57% of spend

Incident **discovery** and **recovery** are the largest elements of internal spend