AT-A-GLANCE



NINTH ANNUAL COST OF CYBERCRIME STUDY

Unlocking the value of improved cybersecurity protection

The Ninth Annual Cost of Cybercrime study combines research across 11 countries in 16 industries. We interviewed 2,647 senior leaders from 355 companies and drew on the experience and expertise of Accenture Security to examine the economic impact of cyberattacks.

THE EXPANDING THREAT LANDSCAPE AND NEW BUSINESS INNOVATION IS LEADING TO AN INCREASE IN CYBERATTACKS

Cybercrime is evolving







Security breaches are growing

Average number Average number of security breaches of security breaches in 2018 in 2017

> Increase in the last 5 years

Technologies introduce risk, and so do humans

of business leaders say new business models introduce technology vulnerabilities faster than they can be secured.

Only 16%

of CISOs say employees in their organizations are held accountable for cybersecurity today.

ORGANIZATIONS SPEND MORE THAN EVER DEALING WITH THE COSTS AND **CONSEQUENCES OF INCREASINGLY SOPHISTICATED ATTACKS**

Cost of cybercrime is rising

cybercrime in 2017

Average cost of

Average cost of cybercrime in 2018

Increase in the last 5 years

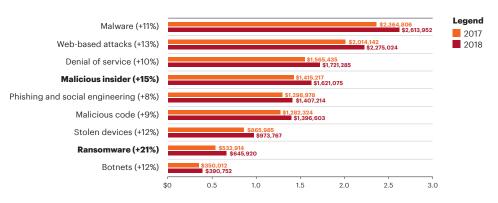
Business consequences are expensive

Cost of business disruption

Cost of information loss

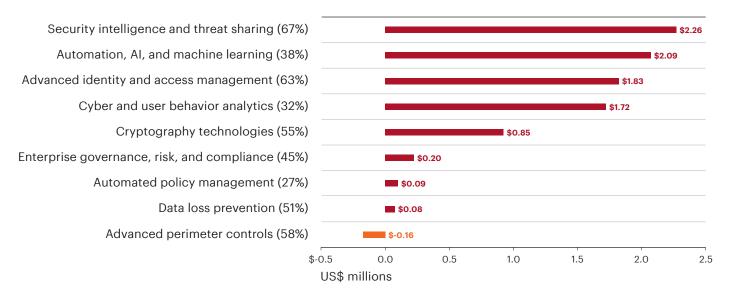
Proportion of spend on discovering attacks in 2018

People-based attacks have increased the most



SECURITY TECHNOLOGIES CAN REDUCE COSTS

Net technology savings (Total technology savings minus total technology spend)



IMPROVING CYBERSECURITY PROTECTION CAN CREATE ECONOMIC VALUE FOR AN ORGANIZATION AND PROVIDE A USEFUL BENCHMARK FOR SECURITY INVESTMENTS

What is economic value?

REDUCE THE COST OF CYBERCRIME

OPEN UP
NEW REVENUE
OPPORTUNITIES

Better cybersecurity protection

IMPROVES COST



INCREASES TRUST



ADDS VALUE \$5.2t

The average G2000 company can gain new economic value

2.8%
Additional revenue

\$580m

THREE STEPS TO UNLOCK CYBERSECURITY VALUE

Prioritize protecting peoplebased attacks



Use training and education to reinforce safe behaviors, for people inside and outside the organization.

Invest to limit information loss and business disruption



Take a data-centric approach to security to better manage information loss and business disruption and comply with new privacy regulations.

Target technologies that reduce rising costs



Use automation, Al/machine learning and advanced analytics to reduce the rising cost of discovering attacks.

^{© 2019} Accenture. All rights reserved. Accenture, the Accenture logo, iDefense and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from iDefense. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.