CANADIAN SECURITY EXECUTIVES HAVE MISPLACED CONFIDENCE IN THEIR ABILITY TO SECURE THE ENTERPRISE

65% of large enterprise security executives have confidence in their cyber security strategies

66% of organizations have completely embedded cybersecurity into their cultures
FAILURE RATES ARE ALARMINGLY HIGH

THOUSANDS to MILLIONS of random breach attempts per week

Nearly 96 focused focused attacks per year, of those, 1 in 3 result in a security breach

That’s 2 to 3 effective attacks per month

Many security breaches go undetected FOR TOO LONG

Detecting a breach takes months for 52% of companies

Internal security teams discover only 65% of effective breaches

Internal breaches are PARTICULARLY PROBLEMATIC

37% say greatest security impact comes from malicious insiders

Yet 1/2 lack confidence in their organizations' internal monitoring

Yet, the survey reveals cybersecurity failure rates are alarmingly high.
CANADIAN EXECUTIVES MUST OVERCOME ERRONEOUS PERCEPTIONS AND FOCUS FOR SUCCESS

START BY ANSWERING THESE QUESTIONS:

- Are you confident that you have identified all priority business data assets and their location?
- Do you have the tools and techniques to react and respond to a targeted attack?
- Do you know what the adversary is really after?
- Are you able to defend the organization from a motivated adversary?
- Do you have the right alignment, structure, team members, and other resources to execute on your mission?
- How often does your organization ‘practice’ its plan to get better at responses?
- How do these attacks affect your business?
INVEST TO INNOVATE AND OUTMANEUVER

Only 1/3 of respondents have confidence in their cybersecurity capabilities regarding any of the 7 domains below, but investment in these areas is critical to improving defenses and strengthening resilience.

1. BUSINESS ALIGNMENT
2. GOVERNANCE & LEADERSHIP
3. STRATEGIC THREAT CONTEXT
4. CYBER RESILIENCE
5. CYBER RESPONSE READINESS
6. THE EXTENDED ECOSYSTEM
7. INVESTMENT EFFICIENCY
REBOOT YOUR CYBERSECURITY APPROACH

PRESSURE TEST SECURITY CAPABILITIES
by engaging “white hat” external hackers to simulate attacks

MAKE SECURITY EVERYONE’S JOB
by fostering a culture of cybersecurity & prioritizing training of all employees

PROTECT FROM THE INSIDE OUT
by prioritizing protection of organization’s key assets

INVEST TO INNOVATE AND OUTMANEUVER,
continually innovating to stay ahead of attackers

LEAD FROM THE TOP
by materially engaging with enterprise leadership & improving the board’s cyber literacy

GROW CONFIDENTLY
by keeping security connected to the bottom line and to real business needs
In 2016 Accenture surveyed 2,000 executives from 12 industries and 15 countries globally, including 124 from Canada.

The survey objective was to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security.

The survey aimed to measure security capabilities across seven cybersecurity strategy domains identified by Accenture: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem.

More than 50 percent of respondents were key decision-makers in cybersecurity strategy and spending, including security, IT and business executives at director level and above at companies with revenues of US $1 billion or more.
THANK YOU

accenture.ca/cybersecurityreport

@AccentureSecure
@AccentureCanada
#CyberSecurity