Accenture Security

HIGH PERFORMANCE SECURITY
REPORT 2016 FOR ENERGY

OUTSIDE THE (BLACK) BOX

PROTECTING CORE OPERATIONS IN ENERGY

ALTHOUGH OIL AND GAS EXECUTIVES EXPRESS CONFIDENCE IN THEIR CYBERSECURITY STRATEGIES OVERALL, 60% STILL VIEW CYBERATTACKS AS A BLACK BOX.

Accenture's 2016 global survey on high performance security reveals several contradictions, among them the difficulty oil and gas companies face when securing their core operations.

3 of 4
respondents express confidence in their abilities to protect their organizations from cyber attacks

63%
say they have completely embedded cybersecurity into their cultures

96
targeted cyber attacks are faced by the average organization per year in the Oil and Gas industry

1 in 3
targeted attacks result in a security breach. That's 2 to 3 effective attacks per month

MANY COMPANIES INVEST INEFFECTIVELY IN CYBERSECURITY...

37 - 61%
would spend extra budget on the same things they're doing now

Only 23%
would invest in mitigating financial loss

Only 23%
would invest in cybersecurity training

Compliance frameworks and programs help define security foundations but don't protect a company from breaches.

REBOOT YOUR APPROACH
DEAL EFFECTIVELY WITH THREATS

1

DEFINE CYBERSECURITY SUCCESS

Improve alignment of cybersecurity strategies with business imperatives and improve ability to detect and prohibit more advanced attacks.

2

PRESSURE-TEST SECURITY CAPABILITIES

Engage 'white-hat' external hackers for attack simulations to establish a realistic assessment of internal capabilities - across IT and OT environments.

3

PROTECT FROM THE INSIDE OUT

Prioritize protection of the organization's key assets (including industrial control systems) and focus on the internal incursions with greatest potential impact.

4

KEEP INNOVATING

Invest in state-of-the-art programs that enable outmaneuvering adversaries vs. investing more in existing programs.

5

MAKE SECURITY EVERYONE'S JOB

99% of breaches not detected by security team members, are found by employees. Prioritize training for all employees, including cross-training for IT and operations personnel.

6

LEAD FROM THE TOP

CISOs must materially engage with enterprise leadership and make the case that cybersecurity is a critical priority in protecting company value.

INVEST TO INNOVATE
AND OUTMANEUVER

INVEST IN YOUR CYBERSECURITY CAPABILITY ACROSS 7 DOMAINS TO IMPROVE DEFENSES AND STRENGTHEN RESILIENCE.

BUSINESS ALIGNMENT
Only 18% of businesses are able to identify high-value assets and business processes.

Understand scenarios that could materially affect the business, identify key drivers, decision points and barriers to strategy development.

GOVERNANCE AND LEADERSHIP
Only 24% of businesses have a clear cybersecurity chain of command.

Focus on cybersecurity accountability, nurture a security-minded culture and create a clear-cut cybersecurity chain of command.

STRATEGIC THREAT CONTEXT
Only 24% of businesses are competent in business-relevant threat monitoring.

Align the security program with the business strategy by analyzing competitive and geo-political risks, peer monitoring and other areas of cybersecurity threats.

CYBER RESILIENCE
Only 22% of businesses have systems and processes that are properly designed in accordance with cyber resilience requirements.

Understand the threat landscape, design key asset protection approaches and use "design for resilience" techniques to limit a cyber attack's impact.

CYBER RESPONSE READINESS
Only 23% of businesses have proper cyber-incident escalation paths.

Develop a robust response plan, strong cyber incident communications, tested plans to protect and recover key assets and effective escalation paths.

THE EXTENDED ECOSYSTEM
Only 24% of businesses are competent at dealing with third-party cybersecurity, **only 24%** are competent at cybersecurity regulatory compliance.

Be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements and focus on regulatory compliance.

INVESTMENT EFFICIENCY
Only 23% of cybersecurity investments protect key assets.

Drive financial understanding of and compare cybersecurity investments against industry benchmarks, organizational business objectives and cybersecurity trends.

BUILD CONFIDENCE
IN THE SECURITY ORGANIZATION

1

Improve overall maturity of the security team and its skills in protecting the business from devastating losses.

2

Improve cybersecurity strategy alignment with business imperatives.

3

Continuously improve your ability to detect and prevent advanced attack scenarios.

FOLLOW US ON TWITTER:
@AccentureSecure

FOR MORE INFORMATION, VISIT:
www.accenture.com/cybersecurityreport

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

171786