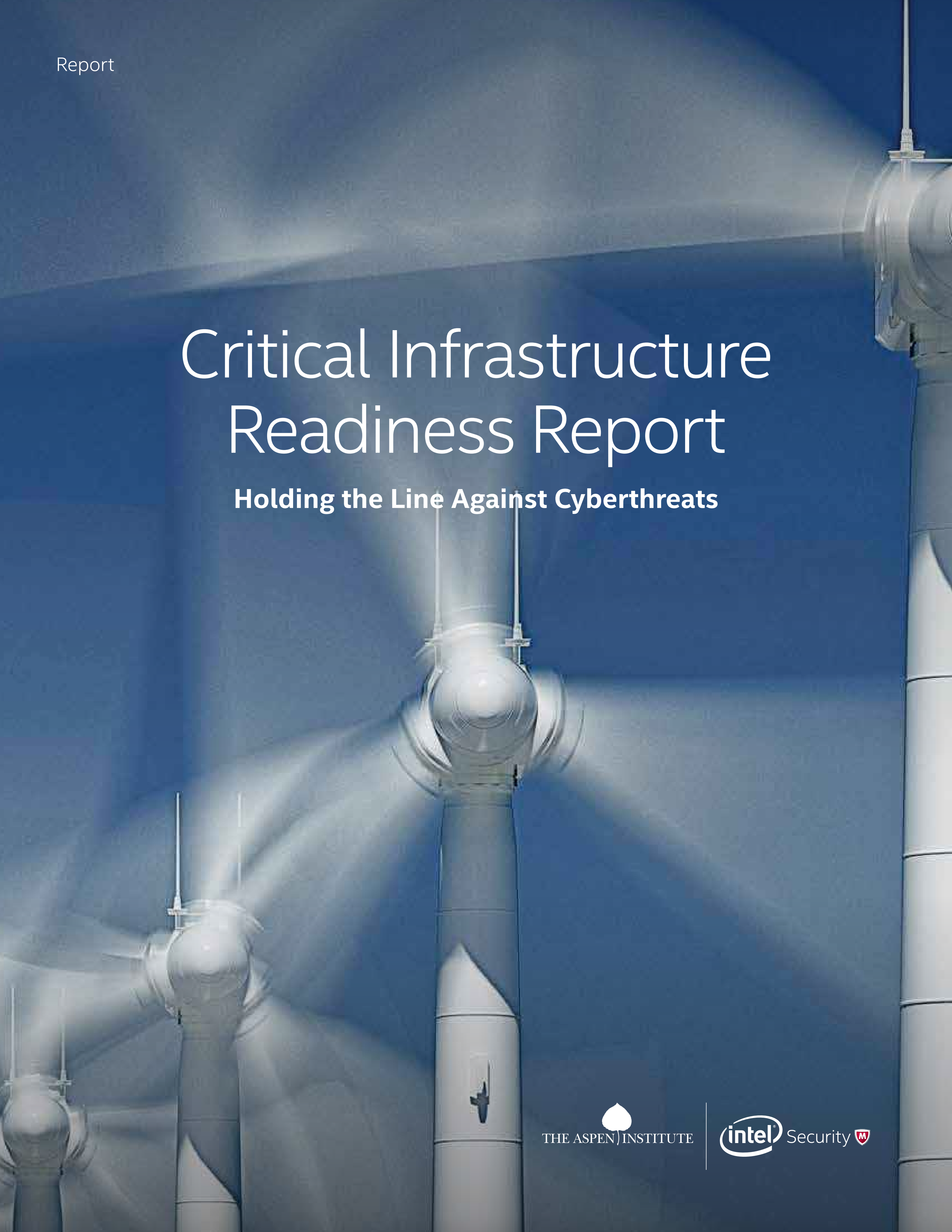
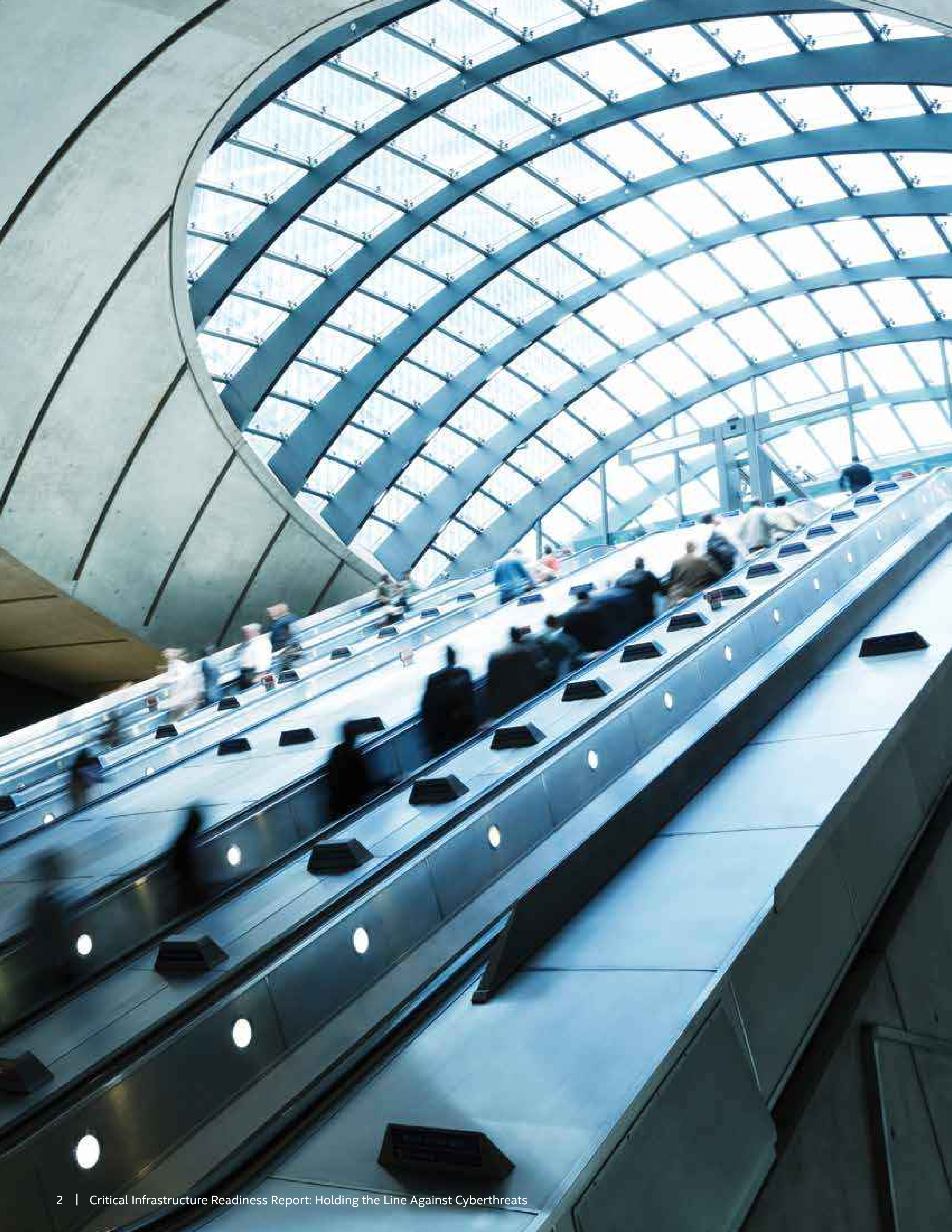
Report



Critical Infrastructure Readiness Report

Holding the Line Against Cyberthreats

THE ASPEN INSTITUTE
intel Security



Executive Summary

Technology and security professionals in North America and Europe profess a great deal of confidence in their cyberdefenses, despite the current spate of high-profile breaches worldwide, according to a new survey made possible by the Aspen Institute Homeland Security Program and Intel Security in advance of the 2015 Aspen Security Forum.

According to McAfee® Labs reports, critical infrastructure organizations are under constant cyberattack, yet no publicly apparent, massive outage has occurred so far. Energy producers, financial services, transportation companies, telecommunications companies, and governments are all potential targets. This report looks at the challenges facing these critical infrastructure organizations in France, Germany, the United States, and the United Kingdom as they work to secure vital systems.

The survey polled information technology and security professionals with an average 12 years of security experience, representing 625 critical infrastructure organizations.* They were asked about their concerns, vulnerabilities, investments, previous attacks, and their interest in cooperating with national and international organizations to improve cyberdefenses. The survey's major findings are below.

Finding 1: Disconnect or overconfidence
Even though major data breaches make regular headlines, many executives surveyed rated their organization's defenses good to excellent, possibly from overconfidence or misplaced faith in their capabilities to effectively respond to an attack, based on Intel Security threat reports.

Finding 2: Threats and confidence both on the rise
The compound annual growth rate of security incidents has increased 66% year over year since 2009.[1] Intel Security saw new ransomware surge 165% in the first quarter of 2015,[1] and, based on the *McAfee Labs Threats Report, May 2015*,[2] Intel Security predicts that the number of cyberattacks launched against organizations and individuals will continue to increase in the coming years. However, most respondents do not appear to correlate these increases with their own vulnerability, and the majority believes their organizations are less vulnerable to attack than they were three years ago.

Finding 3: Favorable to cooperation
More than three quarters of executives believe it is important to increase cooperation among organizations and with their own governments to counter cyberthreats. US, UK, and German companies were the most supportive of this view; those in France were not as convinced, assigning a lower priority to government cooperation.

Finding 4: Serious cyberattack believed likely
Despite high confidence in their own defenses, US and French respondents in particular rate a serious cyberattack affecting critical services and causing loss of life as highly likely within the next three years. Respondents from the transportation and energy sectors were more likely than their counterparts in other sectors to deem the possibility of such an attack "likely or highly likely."

Finding 5: BYOD a non-factor, humans still the weakest link
Few executives believe that the proliferation of personal devices at work is a prime cause of cyberattacks, despite the priority assigned to bring-your-own device issues (BYOD) by cybersecurity companies. Respondents believe user error, not software or device failure, is the leading cause of security breaches.

Defending Infrastructure from Multiple Attack Vectors

An often cited, but still true, statement in cybersecurity is that attackers need to be successful only once. Intel Security's *A Thief□s Perspective*[3] report notes that one of the biggest challenges in defending anything is having to cover every possible attack vector while attackers only need to find one weak point. Whether it is user errors while browsing the web, advanced evasion techniques, slow and stealthy assaults, hidden encrypted infections, or network abuse leading to denial of services, critical infrastructure security cannot leave any of these attack vectors undefended.

Analysis of security incidents at a variety of organizations shows that many of them were breached due to basic security failures in the face of a determined and persistent attacker. This highlights the importance of solid security foundations and implies that it is inappropriate to depend solely on IT-based security.

Finding 1: Disconnect□ Respondents See Decreased Vulnerability Despite News Headlines and Official Policy

At a roundtable discussion at the Aspen Institute in June,[4] White House Counterterrorism and Deputy National Security Advisor Lisa Monaco said the US government sees cyberthreats expanding in every possible dimension—from attack frequency to scale, sophistication, and impact severity. Western critical infrastructure managers in this survey project comparative optimism about their own preparedness, although nearly 80% say cybersecurity in general is either greatly or extremely concerning.

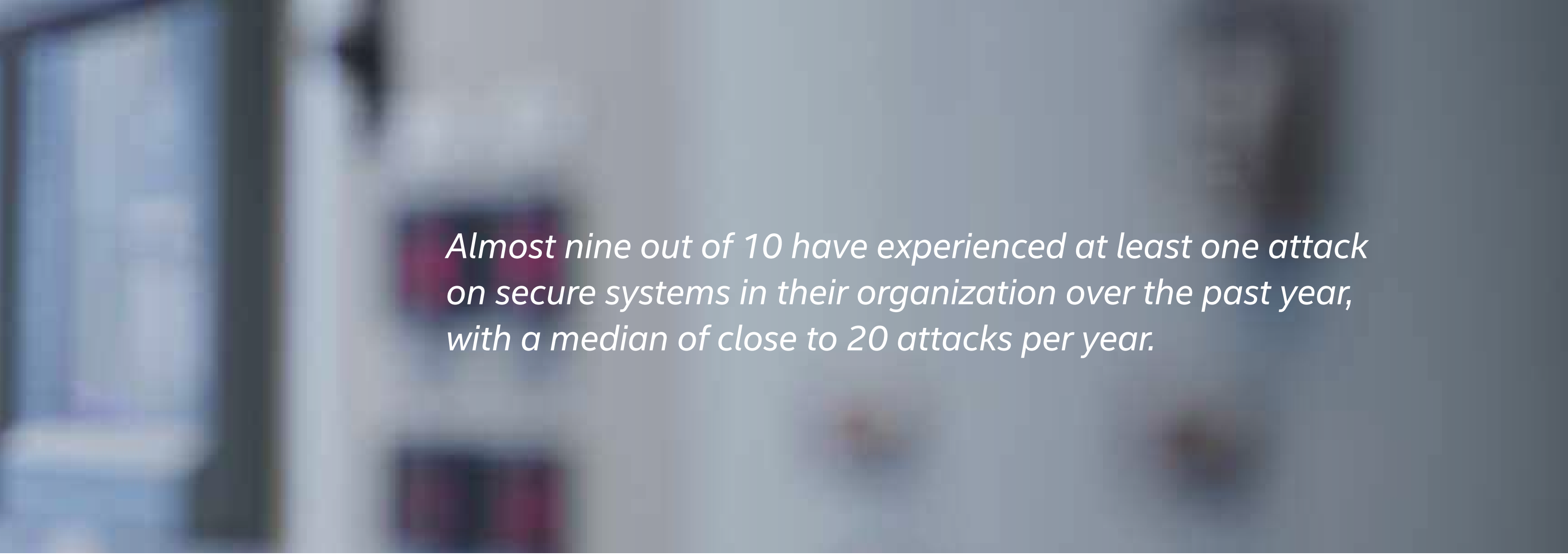
According to the respondents, attack volume is increasing, security breaches are becoming a frequent occurrence, and the rate of code vulnerabilities shows no signs of abating. Yet respondents across all countries and sectors in the survey believe their own vulnerability to cyberattack has declined. When asked how vulnerable their organization is today and how vulnerable it was three years ago, only 27% of respondents reported feeling very or extremely vulnerable today, while 50% stated they felt this way three years ago. Only 8% of respondents feel extremely vulnerable today, down from 12% who felt that way three years ago. The greatest perceived threat among those surveyed is from non-nation state actors: hacktivists, ransomware, and data thieves.

Knowing your enemy helps to prioritize cyberdefenses. According to the standardized threat agent library[5] developed by Intel IT, hacktivists are most likely to attack areas that can disrupt or embarrass the organization. This includes such things as espionage and opportunistic data theft, product alteration, or sabotage. Other attackers, such as terrorists, are more likely to try to cause physical theft, sabotage, or violence.

US respondents report the largest decrease in perceived vulnerability, dropping from 57% three years ago to 24% today, while Germany showed the least change, from 33% to 30%. Financial and transportation organizations reported they felt slightly more vulnerable than average. The energy sector showed the greatest drop over the three years, from 53% to 24%, while transportation showed the least change, from 46% to 31%.

Table 1. Threat agent risk assessment. (Source: Intel® IT Threat Agent Library)

INTENT →	Non-Hostile			Non-Hostile/Hostile		Non-Hostile							
ATTACK TYPE ↓	Reckless Employee	Untrained/Distracted Employee	Outward Sympathizer	Vendor	Partner	Irrational Individual	Thief	Disgruntled Employee	Activist	Terrorist	Organized Crime	Competitor	Nation State
Accidental leak	□	□	□	□	□	□		□					
Espionage				□	□		□	□	□		□	□	□
Financial Faud				□	□		□	□			□		
Misuse	□	□	□	□	□	□		□	□				
Opport. data theft				□	□		□	□	□		□	□	□
Physical theft	□	□				□	□	□		□	□		
Product alteration				□	□			□	□		□	□	□
Sabotage						□		□	□	□		□	□
Violence						□		□		□			



Almost nine out of 10 have experienced at least one attack on secure systems in their organization over the past year, with a median of close to 20 attacks per year.

Finding 2: High Confidence in Existing Security, Although Threat Level Is Increasing

According to news outlets like *The New York Times* and others, many of the attacks in recent headline-grabbing security incidents were under way for weeks or months before initial detection. Yet almost 75% of respondents are confident or extremely confident in their organization's ability to identify cyberattacks. Further, 68% are confident in their ability to mitigate attacks, and 65% are confident that they can deflect them.

At the same time, more than 70% think cybersecurity threats to their organization are escalating, while only 4% think they are in decline. Almost nine out of 10 have experienced at least one attack on secure systems in their organization over the past year, with a median of close to 20 attacks per year. More than 59% of confirmed cyberattacks resulted in physical damage, more than 33% resulted in service disruption, and more than 25% resulted in data compromise, showing that the threats to critical infrastructure are all too real. Those who have endured a higher number of successful attacks and confirmed damage feel more vulnerable than the rest; this suggests that as the number of attacks on all organizations continues to increase, the confidence levels reported in the survey may erode.

A significant majority (84%) of respondents are satisfied or extremely satisfied with the performance of their endpoint protection, network firewall, and secure web gateway solutions. Those who feel less vulnerable than average report that they have invested in more security technologies than the average respondents in the past three years, especially endpoint protection, secure web gateways, and data loss prevention tools. Also, while 48% of them find it likely that a cyberattack will take down critical infrastructure with potential loss of life, 64% believe the reason that has not yet happened is because of good IT security already in place. Only 12% think it is because attack technology is not yet sophisticated enough. With a significant majority of critical infrastructure security professionals expressing a high level of confidence in the security industry's tools and services, the onus is on the industry to make sure they live up to expectations, integrating tools and communications and enhancing industry collaboration.

Finding 3: Favorable to Cooperation□ Support Across the Board for Cooperation, Information Sharing

Private businesses are often uncertain of their government's ability to improve a process or situation. However, critical infrastructure security professionals are open to cooperation with national and international agencies and are confident that their government (68%) and international authorities (60%) can be a valuable and respectful partner. Confidence in their own government agencies was highest in France and lowest in Germany. Confidence in international authorities was highest in Germany and the energy sector, and lowest in US firms, the government, and telecommunications organizations.

Respondents consider cooperation important with their own government (76%), other similar organizations (74%), and other governments (70%), and 86% believe that cooperation between government agencies and private firms on infrastructure protection is critical to a successful cyberdefense. The top three obstacles to greater cooperation are lack of budget, differing approaches to cyberattacks among organizations, and lack of other resources. Firms in the UK, as well as those in the telecommunications and financial services sectors, stated that communicating outside the organization was a bigger barrier than lack of budget or other internal resources.

Respondents were asked about several types of cooperation, such as joining a national or international public-private defense council, sharing network and defense information with other organizations in the same industry or a national or international agency, taking direction from a government agency on cyberdefense strategy, or national legislation on cybersecurity cooperation. The majority of respondents were open to all of these, ranging from 54% open to sharing information with an international authority to 69% open to joining a national defense council. German organizations were consistently most open to these types of arrangements, while those in the UK were consistently least open, 15 to 20 percentage points lower than their German colleagues.

Finding 4: Serious Cyberattack Believed Likely□ US More Worried Than Europe

Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years. US (18%) and French (10%) respondents, in particular, consider this scenario extremely likely. Others did not believe this was likely, with only a few transportation professionals (5%), along with respondents located in the UK (3%) and Germany (2%), thinking that a critical infrastructure takedown is extremely likely.

Finding 5: BYOD a Non-Factor, Humans Still the Weakest Link

Cybersecurity companies consider BYOD and device diversity to be a significant potential attack vector and are encouraging their customers to increase their awareness and defenses against this threat. However, the security professionals surveyed ranked this among the lowest potential causes of successful attacks. Instead, user errors from lack of awareness, use of unofficial online services, and use of social media sites at work were most often ranked as the top three causes. An organization's difficulty in identifying sophisticated threats sometimes made it into the top three and was considered the leading issue for German, UK, and transportation companies.

Critical infrastructure companies have invested in three to four cybersecurity solutions over the past three years on average, with US, UK, and financial services firms reporting above average investment, and French and telecommunications firms reporting below average investment. The most-cited investments were network firewalls, advanced threat detection, intrusion prevention systems, and secure email gateways, while data loss protection, endpoint protection, and security information event management were the least-cited investments.

What to Do

Cybersecurity is an acknowledged national and economic security challenge, but the survey suggests that many IT professionals see themselves as better protected than the infrastructure at large. Interestingly, almost 40% consider themselves no more or less vulnerable than their peers, while 25% believe themselves to be less vulnerable, and 33% think they are more vulnerable. This perception should form the basis for urgent discussion, especially since many enterprise organizations that suffer data breaches may not have, in retrospect, taken all the steps needed to keep defense technologies up to date or make their own employees aware of common, costly error behavior.

The data from this study suggests that security professionals see a need not only for next-generation cyberdefense technology, but also changes in security management, including greater information sharing, closer relationships and cooperation among government and industry, and continued work on basic user threat awareness. Continuing user education about cyberthreats and foundational security practices are essential to help mitigate the user error risk behind many threats, and these are areas where everyone has opportunity to contribute.

Security professionals surveyed are looking to invest in additional command and control functionality to increase their ability to detect threats and attacks. However, this may not be sufficient. While next-generation technologies are increasingly effective, they need to be better linked to adapt and respond to the constantly changing threat environment. An overall security architecture that links protect, detect, and correct functions in a continuously updating cycle improves risk management and is a better match for these new tools.

Government and industry cybersecurity professionals should be pleased by the confidence private organizations place in public defense efforts. But the survey data suggests a level of overconfidence. While the security industry works on next-generation solutions and governments work on sensible legislation, there's still more progress that needs to be made. Adversaries are innovating at a rapid pace, and countering their progress will take much closer cooperation between government and industry. Organizations and government agencies operating in silos do not help the cybersecurity landscape grow more secure. Collaborating with any and all available resources is key to improving the future of security. Reducing critical infrastructure risk is a global strategic challenge, requiring much broader sharing of IT strategies and targeted threat intelligence.

THE ASPEN INSTITUTE | intel Security

About The Aspen Institute

The Aspen Institute is an educational and policy studies organization based in Washington, DC. Its mission is to foster leadership based on enduring values and to provide a nonpartisan venue for dealing with critical issues. Through public and invitation-only forums, roundtables, and conferences, speeches, books, opinion editorials, social media outlets, and media interviews and appearances, the Aspen Institute's Homeland Security Program works to heighten public awareness as to the nation's continued vulnerability to terrorism and to persuade decision makers to take the necessary steps to close the gap between how secure we should be and how secure we actually are. **www.aspeninstitute.org**

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

Individual surveys, such as the one conducted by Vanson Bourne and Intel Security, collect data at a single point in time and thus are not independently able to support long-term conclusions.

***Methodology**

The research, carried out by Vanson Bourne, interviewed 625 IT decision makers with influence over their organization's security solutions. Respondents were from private and public organizations with a minimum of 500 employees, with particular focus on the critical infrastructure sectors of finance (159 respondents), energy (139 respondents), transport (130 respondents), and government (128 respondents). The research was undertaken in the US, UK, France, and Germany. There were 250 interviews conducted in the US and 125 in each of the other countries. The full data set is available on request

[1] www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml

[2] *McAfee Labs Threats Report, May 2015*, www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf

[3] www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf

[4] www.aspeninstitute.org/video/future-cyber-threats-featuring-lisa-monaco

[5] https://communities.intel.com/docs/DOC-1151