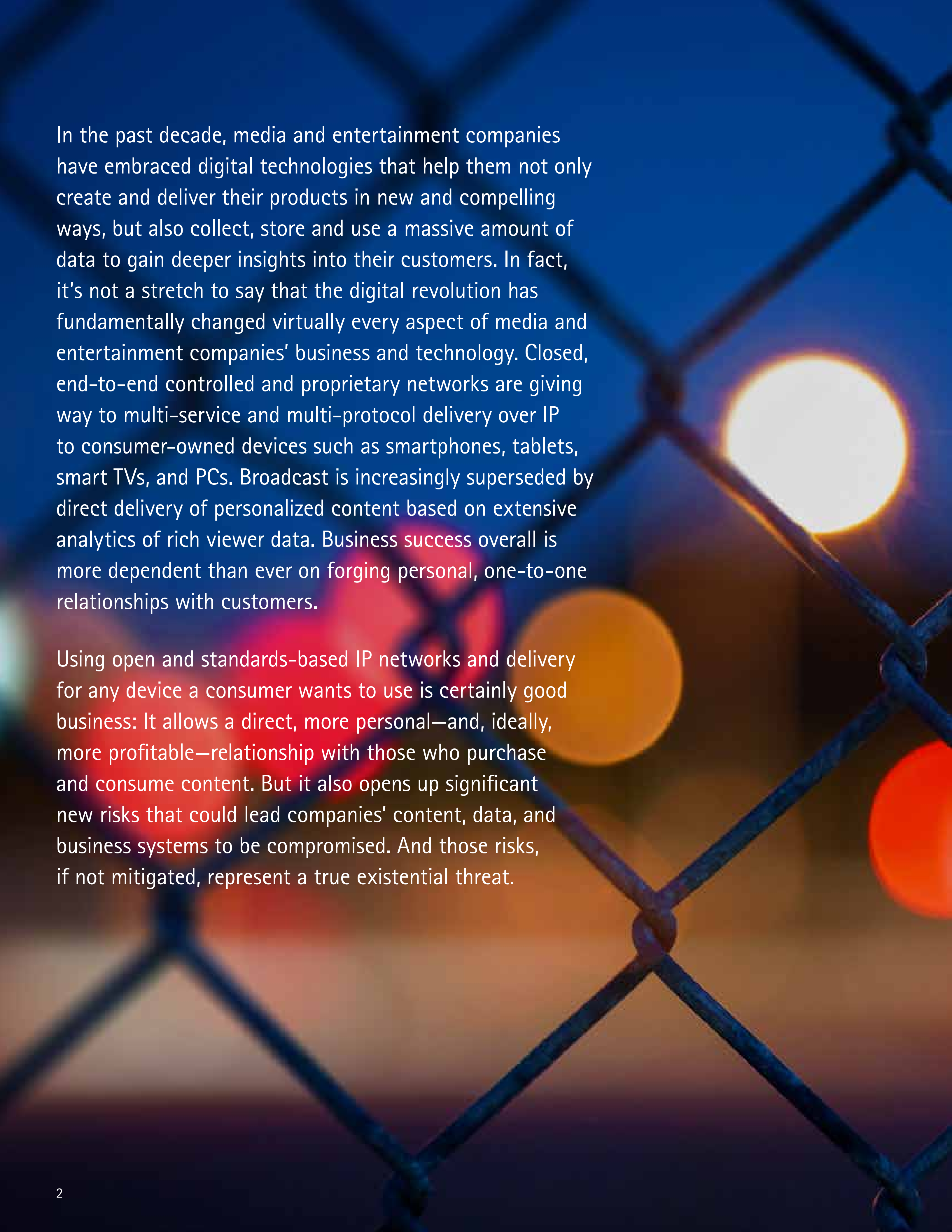
accenture operations

The New Security Challenge

Are Media & Entertainment Companies Ready?

High performance. Delivered.

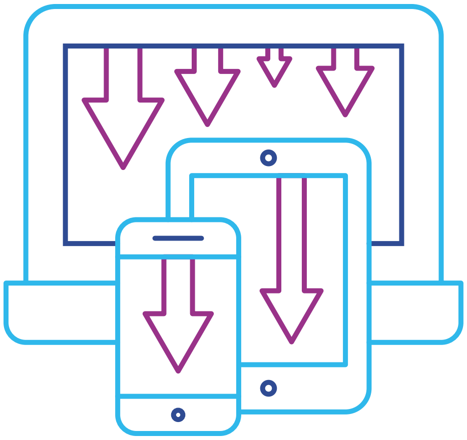
Strategy | Consulting | Digital | Technology | Operations



In the past decade, media and entertainment companies have embraced digital technologies that help them not only create and deliver their products in new and compelling ways, but also collect, store and use a massive amount of data to gain deeper insights into their customers. In fact, it's not a stretch to say that the digital revolution has fundamentally changed virtually every aspect of media and entertainment companies' business and technology. Closed, end-to-end controlled and proprietary networks are giving way to multi-service and multi-protocol delivery over IP to consumer-owned devices such as smartphones, tablets, smart TVs, and PCs. Broadcast is increasingly superseded by direct delivery of personalized content based on extensive analytics of rich viewer data. Business success overall is more dependent than ever on forging personal, one-to-one relationships with customers.

Using open and standards-based IP networks and delivery for any device a consumer wants to use is certainly good business: It allows a direct, more personal—and, ideally, more profitable—relationship with those who purchase and consume content. But it also opens up significant new risks that could lead companies' content, data, and business systems to be compromised. And those risks, if not mitigated, represent a true existential threat.

Exposing the Downside of Digital



The fact is, exploding new and unfamiliar risks, combined with a spate of high-profile security breaches, have made security a board-level issue and a major focus for companies' senior leadership. In one Accenture survey, for example, more than half of participants said security concerns are one of their biggest challenges in digital technology implementations.[1]

How has the security landscape changed?

New and Different "Attack Surfaces"

For starters, the industry's shift to digital introduces entirely new classes of threats. Before the digital era, companies operated proprietary and closed systems with controlled distribution. Akin to bulwarks —they were extremely hard to attack, and even harder to penetrate, without expensive and hard-to-get equipment.

Then the Internet came along with its own set of freely available and powerful tools that can be used for nefarious purposes. Further, many new systems are deployed, partly or wholly, in the cloud. The cloud, of course, makes new and attractive business models and delivery options more compelling. But it also exposes new weaknesses and attack avenues, thus fundamentally changing the security model needed to keep things safe.

Other new surfaces that are attractive to attackers include systems such as digital analytics and content supply chains.

Richer Targets

The data explosion accompanying the digital economy, in itself, has created a new and valuable asset. In particular, newly collected personal data is vital to crafting and delivering the personalized experiences consumers clamor for—and, in many cases, are willing to pay more to get. However, that data is also irresistible to cyber criminals. Personal data is a commonly traded commodity; its value in the "underground economy" can range from a dollar or two for a stolen credit card number to as much as $1,000 for a more comprehensive cache of personal data.[2] The content remains a prime target as well. Hackers may be interested in stealing, destroying or exposing a company's content (such as movies or any products delivered to end users) as well as other related intellectual property such as scripts.

Depth and Breadth of Impact

As more media companies transform into truly digital businesses, their technologies and the data running through them become the business. Thus, any security breach could have a much greater impact than it would on a company less reliant on its digital assets. Leaders of digital businesses are rightly concerned about the myriad of threats that could inflict substantial harm on their companies and customers. According to an Accenture survey[3] of enterprise security professionals, insider corporate data theft and malware infections are among the biggest threats to digital businesses. Over four in 10 survey participants are strongly or critically concerned about theft of corporate information and just under half are similarly concerned about theft of personal information. And 77 percent of respondents at media and technology companies said their company experienced an attempted or successful theft or corruption of data by insiders during the prior 12 months.

New Classes of Attackers

The richer targets and increased impact provide motive, while the new threats and attack surfaces offer the opportunity. The combination has spawned a toxic global stew of shadowy operators poking and prodding networks in the hope of a big score. The rarefied ranks of attackers skulking on the closed proprietary networks of the past are still around, but they're now joined by a whole range of newcomers: Cyber criminals, script kiddies and kudos hackers, hacktivists, terrorist organizations, and even nation states may join the fray, each for their own reasons.

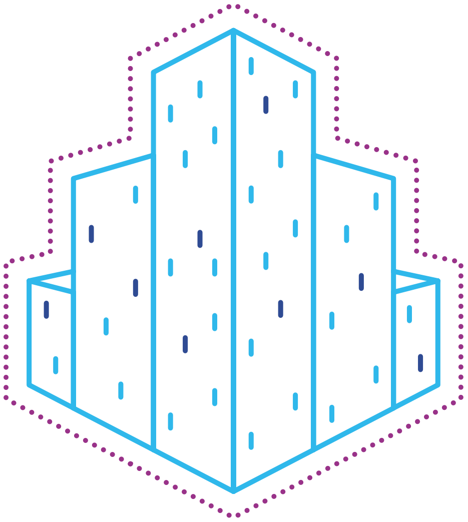
All of the above would be concerning even if it were mere theory. But as we all know, it's not. It's very real, as several media and entertainment firms have already experienced in succumbing to high-profile and high-impact attacks.

Sony Pictures Entertainment is one of them. The company was hacked very publicly and repeatedly, leading to compromise of 77 million customer records, unpublished movies, and internal confidential information.[4] Attacks on global television network TV5 Monde took 11 stations off the air temporarily and hijacked the company's social media accounts.[5]

And these are not isolated incidents. The 2016 Verizon Data Breach Investigations Report counted 232 security incidents in 2015 – with confirmed data losses in entertainment and information industries.[6] Akamai recorded more than 40M web application attack triggers in media and entertainment industries in the first quarter of 2016 alone.[7] In the face of so many attempts, companies cannot afford to bury their heads in the sand and hope it all goes away. It won't. If anything, it's only going to get worse. That means more action is called for to reduce the risk of becoming a victim of high-impact attacks.

Yet at the same time, the amount of money companies spend to protect themselves against breaches continues to rise. In fact, the cost of attacking versus the cost of defending clearly favors the attackers. Companies need to find a way to marshal their resources most effectively to keep attackers at bay.

Building a Holistic, Business-Focused Cyber Defense Approach



Fortunately, the same digital trends that put businesses at risk also gives rise to tools that more cost-effectively manage that risks and address new digital security challenges.

Such tools should be at the heart of a holistic, 360-degree approach to security that relentlessly focuses on business impact – an understanding of the benefits to getting it right and the potentially dire consequences of getting it wrong.

This approach (Figure 1) begins with laying the groundwork that prepares a company to do battle against those intent on doing it harm. Among the key elements of this groundwork are robust security strategies that tightly align with the business; a detailed understanding of the company's current security posture and where it needs to be; the appropriate governance to ensure security is enacted properly and consistently; and the rooting of a security mindset in the company's culture and people to make security second nature.

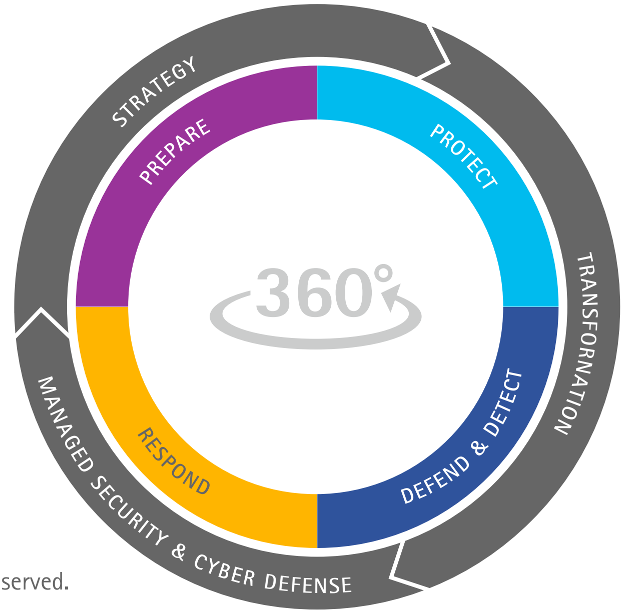
This serves as the foundation for the steps a company subsequently should take to protect its business from threats. Virtually all companies have put in place, to varying degrees, measures to keep their data and systems secure. This includes securing the company's applications, data, and infrastructure, but also managing digital identity for people connected to the business, such as employees, contractors, partners, and consumers.

But more than ever, security should extend beyond putting in place protection. Sound application, platform, and infrastructure security – while vital – is no longer sufficient. There are myriad ways an attacker can overcome even the best-laid protection. Human error, malicious insiders, bugs and vulnerabilities, privilege escalation, and lateral movement from associated systems are just a few examples. Therefore, additional steps are needed.

Figure 1: Companies need a holistic, 360-degree approach to security in the face of new threats.

- Strategy & Business Alignment
- Assessment & Architecture
- Governance, Risk & Compliance
- People & Culture Change

- Application & Data Security
- Platform & Infrastructure Security
- Digital Identity



- Incident Responses
- Remediation

- Vulnerability Management & Threat Intelligence
- Advanced Adversary Simulations
- Security Monitoring
- Cyber Threat Analytics

First, a company should embrace ongoing defense and detection, as it's a matter of when, not if it will experience an intrusion.

Defense

Defense consists of threat and vulnerability management, which help shore up existing protection measures or speed up detection and remediation if vulnerabilities exist that can't be fixed promptly. Another defensive action is threat intelligence, which alerts the right people within the company (with actionable advice) if attacks happening could escalate and impact other parts of the company. Advanced adversary simulation takes the penetration test to the next level: It raises the bar by simulating a determined, capable, and targeted attacker, consisting of techniques such as social engineering.

Detection

Detection enables a company to know when and how it was attacked and when its protection has been breached. This may seem obvious, but the numbers suggest otherwise: According to several independent reports, more than half of all security breaches are detected not by the victim but by third parties. Worse, the average time of detection is measured in months—a timeframe that offers attackers, who typically need only a few days to reach their objective, plenty of time to wreak havoc. Therefore, detection should include deep and broad monitoring capabilities as well as fast and reliable analytics. The latter helps focus a company's scarce security resources only on genuine security incidents that may have real, substantive impact, and not waste their time on an endless series of false positives.

Finally, today's security approach should incorporate a structured incident response that's a formal capability embedded throughout all stages—not a standalone activity run by a single function such as IT. In the event of an incident, the business must be fully involved in deciding how to keep systems running, reduce the impact, and apprehend the attackers. In many cases, the communications and legal functions will play key roles in response. Intuitively, response must cover containment and recovery of any incidents. But equally important, it also should include processes to improve protection, defense, and detection based on the past experiences to reduce the potential of similar outcomes in the future.

The preceding intuitively require top-notch security capabilities—that's a given. But the assets that need protection—as well as the attackers, threats, vulnerabilities, and potential business impact—vary from company to company. That's why building a robust, comprehensive and effective approach to security also requires a deep understanding of the business. Such knowledge is key to being able to accurately define what the company is up against and secure the organization's assets accordingly.

Now's the Time to Boost Efforts to Safeguard Digital Assets

The rallying cry for businesses over the past decade clearly has been "Go digital!" And few industry sectors have taken that to heart as media and entertainment. Such companies are using digital technologies to fundamentally change not only their business models, but also their offerings, to uncovering new growth opportunities. In the process, they're charting the course toward the future of media and entertainment, which is decidedly digital.

But they're also becoming more vulnerable to threats—which continue to proliferate as new players get into the act and potent new tools emerge that can make it much easier to penetrate a company's defenses. That's why it's more critical than ever for media and entertainment companies to step up their efforts to safeguard their digital assets with a new, holistic approach to security that's tailored to the unique context in which such companies operate, and that can keep pace with the ever-growing frequency and sophistication of attacks. Doing so is vital to not only their competitiveness, but also to their very survival.

Reference

1 "Growing the Digital Business: Accenture Mobility Research 2015"

2 "Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers," Tim Greene, Network World, February 6, 2015. http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

3 "New Report Finds Insider Corporate Data Theft and Malware Infections Among Biggest Threat to Digital Business in 2016," Accenture news release, June 27, 2016. https://newsroom.accenture.com/news/new-report-finds-insider-corporate-data-theft-and-malware-infections-among-biggest-threat-to-digital-business-in-2016.htm

4 "Hack of the Century," Peter Elkind, Fortune, July 1, 2015. http://fortune.com/sony-hack-part-1/

5 "Cyberattack disables 11 French TV channels, takes over social media sites," Don Melvin and Greg Botelho, CNN, April 9, 2015. http://www.cnn.com/2015/04/09/europe/french-tv-network-attack-recovery/index.html

6 "2016 Data Breach Investigations Report," Verizon, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

7 "Q1 2016 State of the Internet—Security Report," Akamai. https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

Authors

Brian Ward
Communications, Media and Technology
NA Technology Security Lead

Ganesh Devarajan
Communications, Media and
Technology Central US Security Lead

Peter De Rooij
Communications, Media and Technology
UK Security Principal

Sanjeev Shukla
Communications, Media and Technology
UK Security Lead

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 375,000 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.

For more information on Accenture Security Services please visit http://www.accenture.com/cybersecurity