Connect to People

How people use technology matters. Knowing the risks of texting while driving or how to use the Internet safely at any age can help us make better choices. Learn how we're helping to meet the diverse needs of technology consumers and fostering a workplace that supports all employees.

Network Security

Materiality Assessment Topic: Network and data security | Global Reporting Initiative Standard Disclosures: GRI 418-1, Network and data security MA

Issue Summary

Information and communications technology networks are key parts of our everyday lives, enabling transactions and communication between individuals, businesses, governments and others. As we increasingly depend on networks to carry more information, they must remain reliable and highly secure. Attacks on networks and Internet of Things (IoT) devices can include viruses, worms, denial-of-service, ransomware and phishing.

Our Position

AT&T operates one of the world's most advanced and powerful global backbone networks. With more than 200 petabytes of data crossing our network every day, we analyze approximately 686 billion flows that represent 19 petabytes of data per day. Security is at the core of our network and central to everything we do.

Our Action

The world of networked computing—especially for today's mobile and always-connected IoT devices and applications, as well as cloud environments—is fast-moving and highly dynamic. As a result, AT&T is continually improving security through active research and development programs, influencing (via standards organizations) and tracking of industry developments, and the evaluation of new security technologies and products. AT&T is constantly employing new tools and systems to deliver highly effective security safeguards.

AT&T Chief Security Office (CSO)

The CSO serves as the lead for the corporation, but a focus on security has been built into the fabric of every organization within the business. The CSO maintains a global security organization comprised of more than 600 security professionals, and more than 1,400 additional security specialists work in other organizations across AT&T. The CSO is dedicated to the

protection of the AT&T global network. It supports a broad range of functions, from security policy management to security solutions. Additionally, the group reviews and assesses our security control posture to keep pace with industry developments and to satisfy regulatory and business requirements.

At the executive level, the AT&T chief security officer leads the AT&T Security Advisory Council, a program through which key business and functional leaders meet on a regular basis to discuss corporate security strategy, vision and concerns. The CSO's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities and assess compliance with security best practices. Additionally, the audit committee of the board of directors oversees the AT&T risk management strategy, which includes cybersecurity and defense of our network.

AT&T Security Standards

AT&T has developed and maintains the AT&T Security Policy and Requirements (ASPR), a set of security control standards based in part on leading industry standards such as ISO/IEC 27001:2013. ASPR aligns to laws and standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST 800-53. AT&T also performs annual 3rd-party certifications/audits, such as the Payment Card Industry, Sarbanes-Oxley Act (SOX) and SSAE 16/ISAE 3402 (SOC), to demonstrate compliance to our customers and our stakeholders.

Given the dynamic environment that AT&T supports, ASPR content is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, operating procedures, tools and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout our company. ASPR applies enterprise-wide and establishes the minimum required safeguards to protect computing and networking assets, data and services. It applies to all employees, contractors, supervisors, application/software developers, system and database administrators, network architects and operations teams.

AT&T maintains global ISO 27001 certification, which includes the information security management systems (ISMS) for the AT&T global IP network and customer-facing services.

AT&T is compliant with Europe's comprehensive privacy and data protection–strengthening law General Data Protection Regulation (GDPR), which became effective on May 25, 2018. Many data protection features of the GDPR are also found in the privacy laws of other countries around the world. As such, the AT&T Privacy Office is leading and has prioritized global interoperability as part of a global privacy strategy. As a result, a new category of sensitive data was created in which AT&T has pre-defined the elements for restricted personal information (RPI), which apply across the entire AT&T enterprise—essentially, AT&T employees and non-payroll workers living in the EU and our customers. Additionally, AT&T proprietary information

(sensitive personal information or SPI) related to the provision and administration of AT&T services is accorded significant protections. Certain customer information managed by AT&T is further protected by a Privacy Policy applicable to all employees and contractors and a Code of Business Conduct that assigns penalties for violation of the duty to protect the confidentiality of SPI and other sensitive data. As appropriate, the CSO coordinates and assists the company's privacy team on data breach investigations and the company's Asset Protection group (also known as Corporate Security) on issues pertaining to the protection of company personnel, property and other assets.

Training and Compliance

The AT&T CSO is charged with directing and coordinating security awareness and education across AT&T. The group maintains an internal security awareness website, an internal awareness newsletter, employee- and business unit–specific bulletins and communications, job aids, technology conferences and employee security awareness events to deliver general and targeted security awareness initiatives within AT&T. The program uses subject matter experts from the various security groups and disciplines for content development and to deliver webcasts and video productions.

The AT&T internal security awareness program takes an innovative engage-while-learning approach. Our program enforces personal responsibility from every person who touches the network—from office workers and server administrators to folks in the field and more. Using a series of animated characters to share learnings about security, the storylines ask employees to imagine real-life scenarios that could involve them such as opening a dangerous link or sending data unencrypted. Our character—which has become an iconic internal brand—learns awareness lessons on behalf of the employee.

Under the banner of the AT&T proprietary slogan You Are the Firewall^{SM}, these animated short stories, original video games with embedded security training, live game shows and an International Security Awareness Week promote security with employees at all of our world-wide AT&T locations. This entertainment approach to the security awareness program was reviewed by industry analysts and has received the highest acclaim from the Institute for Applied Network Security.

The AT&T Chief Security Office also produces a weekly security program featuring AT&T Chief Security Office analysts. AT&T ThreatTraq adds another dimension of security training and awareness through its weekly webisodes, featuring CSO security analysts and open to the public on the internet.

All AT&T employees are required to annually acknowledge their responsibility to adhere to our Code of Business Conduct and our information security policy. AT&T employees receive periodic awareness and compliance training to reinforce our privacy standards.

We encourage employees to obtain security training and achieve accreditations and certifications when relevant. This training is conducted both within AT&T and through corporate training organizations such as:

- The International Information Systems Security Certification Consortium, or (ISC)²
- The Information Systems Security Association
- The SANS Institute
- Vendor- and product-specific training and certification

Our large population of security professionals maintains certifications and credentials such as:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)

AT&T conducts regular reviews of our operations and applications for security compliance, which is essential for evaluating adherence to our security procedures. These reviews may be facilitated or conducted through our CSO; by a business area sponsor of a product, service, supplier or partner relationship; or by an operations team responsible for lifecycle service management.

Testing and Reporting

AT&T conducts regular tests and evaluations to help ensure that security controls are maintained and functioning in accordance with our security policy. Security status checking includes:

- Reviewing and verifying system security settings, computer resource security settings and status, and users having security administrative authority or system authority;
- Testing of network elements to ensure the proper level of security patches and that only required system processes are active; and
- Validating server compliance with the AT&T security policy.

Vulnerability testing is performed by authorized personnel, using AT&T-developed tools and leading-edge scan tools, to verify whether controls can be bypassed to obtain any unauthorized access. We use systemic anomaly reporting to indicate abnormal use of our online customer relationship management (CRM) systems, both customer facing and employee facing. These alarms are investigated and appropriate remediation steps are taken.

Information regarding the security of our infrastructure and services is managed and communicated on a need-to-know basis. Results of our testing and checking are combined with threat intelligence gathered through trend analysis and reported to security organization executives.

Additionally, AT&T uses a consistent, disciplined global process for the timely identification of security incidents and threats. The AT&T Global Technology Operations Center (GTOC) maintains 24/7, near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. Our threat management platform and program provide near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trending analysis and predictive security alerting.

We also encourage and reward contributions by developers and security researchers who make our online environment more secure. Through the AT&T Bug Bounty Program, we provide monetary rewards and/or public recognition for security vulnerabilities responsibly disclosed to us.

AT&T Security Research Center

The AT&T Security Research Center was created within the AT&T CSO to invent the future of security in communications and computing, and to create what may be impossible today and revolutionary for tomorrow. Researchers work on large-scale problems in areas such as mobility and cellular, cloud computing, networking and data mining. In particular, they look for ways to leverage the power of the network for new security architectures and mechanisms.

AT&T Business Solutions

AT&T is helping enable businesses to detect, analyze and address security threats faster and more efficiently than ever before. AT&T Threat Intellect^{SM} provides unparalleled visibility into the data patterns and threat activity across our network, helping businesses customize their security to meet their needs. It uses multitudes of unique threat signature data streams, analytics and intelligence to help detect known and unknown threats. Threat Intellect is also constantly learning to adapt to the latest global security issues.

Business Continuity and Disaster Recovery

The AT&T Business Continuity Management Program is certified to the international business continuity standard ISO 22301:2012. It is also aligned with the Disaster Recovery Institute International (DRII) Professional Practices, Business Continuity Institute Good Practice Guidelines, Department of Homeland Security National Incident Management System and ISO 31000. These standards demonstrate that AT&T continues to be equipped to resume business

operations and continue delivering services to our customers in the vital hours and days after a disaster strikes. In the event of any disaster or other emergency, we will be able to quickly resume network traffic, field customer calls and queries, and service the communities in which we operate. The AT&T Business Continuity Management Program includes management disciplines, processes and techniques to support our essential business processes in the event of a significant business disruption. For more information, visit AT&T Vital Connections and read our Disaster Response issue brief.

Engaging with Stakeholders

AT&T is proud to be a leader and a participant in many industry, academic and governmental organizations both to set standards and to keep pace with industry developments. Our employees interact with and participate in several U.S. and international security organizations, including:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- Forum of Incident Response and Security Teams (FIRST)
- National Security Telecommunications Advisory Committee (NSTAC), a federal advisory council to the president of the United States on issues of national security and emergency preparedness
- National Coordinating Center for Communications (NCC), which serves as the Information Sharing and Analysis Center (ISAC) for communications and organizes operational response activities in the event of both cyber and physical incidents
- Communications Sector Coordinating Council (CSCC), which conducts planning activities on cybersecurity issues with the U.S. Department of Homeland Security
- U.K. Centre for the Protection of National Infrastructure (CPNI) National Security Information Exchange (NSIE)
- Various Information Sharing and Analysis Centers (ISACs), including the Information Technology, Auto and Retail ISACs
- U.S. InfraGard
- Security activities within the Internet Engineering Task Force (IETF)
- National Cyber Security Alliance (NCSA), which conducts cybersecurity awareness campaigns targeted toward consumers, K-12 students and small businesses

AT&T also participates in:

- National Infrastructure Protection Center (NIPC)
- National Telecommunications and Information Administration (NTIA)
- Federal Communications Commission (FCC) Communications Security, Reliability and Interoperability Council (CSRIC)
- Network Reliability Steering Committee (NRSC)

- USTelecom and the Council to Secure the Digital Economy (CSDE)
- Cellular Telecommunications Industry Association (CTIA) cybersecurity working group
- Consumer Technology Association (CTA) technology council security working group
- National Institute of Standards and Technology (NIST) and the Internet Security and Privacy Advisory Board (ISPAB)
- Internet of Things (IoT) Cybersecurity Alliance (IoTCA)

AT&T security experts gather weekly to provide information and perspective on the latest security news and trends through our AT&T ThreatTraq channel. Visit our network security services page for more information about our offerings for customers and our public policy blog, which offers our view and commentary on cybersecurity policy news.

Awareness and Education

Education is the best line of defense. As more devices connect to the internet, this becomes more important. Cyber Aware is a new resource from AT&T to empower and educate consumers about fraud protection and cybersecurity. Our goal is to make customers more alert to help them protect their information. We recognized that many customers have questions, but they did not know where to find answers. The site explains in simple terms how many scams work, ways to recognize them and things customers can do. It offers security and privacy alerts that provide advice on patches and updates. It's available to everyone—not just AT&T customers—at att.com/cyberaware.