MANAGING CYBER RISKS

ACROSS THE SOFTWARE SUPPLY CHAIN

Managing Cyber Risks Across the Software Supply Chain

The widespread deployment of advanced data communications technologies is a vital factor in today's global economy. But it has also created a pathway for bad actors to gain access to systems that were assumed to be secure, enabling them to breach proprietary or confidential information or to control essential operations. As the risk of cyber threats continues to increase, cybersecurity has become a key consideration for both organizations and individuals.

Critical infrastructure type industries and other large entities are especially vulnerable to cyber breaches that can compromise data privacy and security. This is especially the case with third-party software, such as open source software, vendor-provided software or snippets of code taken from online sources. Since more than 80 percent of software applications available today are comprised of open-source components[1], organizations must be especially vigilant to implement rigorous software supply chain management systems and procedures to mitigate the potential risk from third-party applications.

This UL white paper will discuss the importance of validating the security and integrity of the software supply chain, and the benefits of adopting a common set of technical criteria that can be verified by an independent third-party. Beginning with a summary of recent examples of high-profile cyberattacks attributable to software vulnerabilities, the white paper then presents an overview of some of the general cybersecurity risks in supply chains of critical infrastructure industries, with special attention to software supply chain issues. The paper then discusses steps that asset owners can take to mitigate potential vulnerabilities attributable to software, and concludes with a discussion of UL's Cybersecurity Assurance Program (CAP) and the UL 2900 series of standards.

Cybersecurity and the Critical Infrastructure

A principle focus of efforts to protect against cybersecurity threats has been on those entities that are considered part of the critical infrastructure. The critical infrastructure can be defined as "IT assets, networks, services and installations that, if disrupted or destroyed, would have a serious impact on the health, security or economic well-being of citizens and the efficient functioning of a country's government[2]." Industries most often designated as part of the critical infrastructure include defense, energy generation and distribution, water systems, transportation and shipping, financial services, healthcare and public safety.

Predictably, the central role of critical infrastructure industries in day-to-day life means they represent an attractive target for Cyberattacks. The Industrial Control System Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security estimates that 295 incidents involving cyberattacks against critical infrastructure operations were reported in the U.S. in 2015, a 20 percent increase from the 245 incidents reported in 2014[3]. Cyberattacks reported in connection with manufacturing operations accounted for a third of all reported incidents (97), followed by energy sector entities (46 incidents, or 16 percent) and water systems operations (25 incidents, or 9 percent).

Because of their overall importance, entities that work within designated critical infrastructure industries are expected to comply with mandated or recommended cybersecurity requirements and practices. In the European Union (EU), for example, the European Programme for Critical Infrastructure Protection (EPCIP) focuses on critical infrastructure entities within the transportation and energy industries and details specific requirements applicable to entities within those industries. These requirements include the development of an operator security plan that identifies important infrastructure assets, provides a detailed threat assessment based on asset vulnerability, and details countermeasures to combat cyber threats. Some EU Member States, including Germany and the United Kingdom, have additional cybersecurity requirements applicable to critical infrastructure entities.

In the U.S., some critical infrastructure industries have adopted polices and requirements to protect against cyber threats. For example, the North American Electric Reliability Corporation (NERC) has issued a number of mandatory reliability standards for critical infrastructure power companies, including reliability standards that address protection against cyberattacks[4]. And chemical facilities are subject to risk-based performance standards developed by the U.S. Department of Homeland Security to protect against potential terrorist threats, including cyberattacks[5].

At the federal level, Presidential Executive Order 13636 (Improving Critical Infrastructure Cybersecurity)[6] was issued in February 2013, and called on the National Institute of Standards and Technology (NIST) to develop risk-based cybersecurity measures and practices that could be adopted by entities designated as part of the critical infrastructure. The resulting Cybersecurity Framework[7], published by NIST in 2014, provides general guidance for reducing cyber threats based on existing standards, guidelines and practices. But, for many critical infrastructure entities, the Framework may lack the additional prescriptive requirements needed for evaluating products being purchased, how to test those products and the expected results.

Supply Chain Software Vulnerabilities

For entities in critical infrastructure industries, one of the more pernicious but less often identified causes of cybersecurity breaches can be found in third-party software purchased or downloaded for use in internal systems and operations or for integration into finished goods. In recent years, developers have increasingly turned to off-the-shelf software components as an effective way to speed the development of software and applications. At the same time, the most commonly used software products, including webservers, Internet browsers, communications and encryption libraries come from established third-party software vendors.

Unfortunately, while third-party software components can help to increase development productivity and even result in better product quality, their expansive use has also introduced new cybersecurity risks, leaving critical infrastructure industries even more vulnerable to cyberattacks. Without adequate systems and procedures in place to evaluate and control third-party software and components sourced from the software supply chain, organizations may unknowingly use or integrate software into operational systems or end products with insufficiently robust security that can be easily hacked or otherwise compromised.

In the past two years alone, there have been a number of high-profile examples of how software vulnerabilities can lead to major consequences for entities in critical infrastructure industries.
Specific instances include:

- In a series of attacks in 2014 and 2015, personnel records of more than 21 million current and former U.S. federal employees and federal contractors were illegally accessed on computers systems maintained by the U.S. Office of Personnel Management (OPM). The hacked information reportedly included social security numbers as well as detailed data and fingerprints of approximately five million employees and contractors who had been granted security clearance for access to sensitive information[8]. A report by the OPM's Office of the Inspector General had previously identified "significant" deficiencies in the department's IT security systems and protocols[9].

- In December 2015, hackers successfully shut down three regional power companies in Ukraine in a coordinated attack that left hundreds of thousands of people without electrical power. The hackers reportedly took remote control of the plants' breaker systems using remote administration tools at the operating system level or remote industrial control system client software via the plants' virtual private network (VPN) connections[10].

- Files of approximately 15 million applicants who applied for credit with T-Mobile USA were breached in October 2015. The processing of T-Mobile credit applications was handled by Experian, the world's largest credit monitoring firm. Its credit information support portal reportedly permitted the uploading of application attachments without first requiring users to provide validated credentials, giving hackers an easy path for the introduction of malware[11].

- In February 2015, computer systems at Anthem, the second-largest healthcare insurer in the U.S., were attacked, compromising an estimated 80 million patient and employee records. Exposed information included patient and employee names, dates of birth, social security numbers, income data and private contact information[12]. According to an Anthem spokesperson, patient and employee data stored on the company's computers was not encrypted[13].

- In late 2014, hackers took control over production systems at a steel mill in Germany, remotely manipulating control systems to prevent the plant's blast furnace from being shut down. According to a report issued by Germany's Federal Office for Information Security (BSI), the hackers accessed the plant office's software network and then used that access to gain control of the plant's production management software. As a result, the plant reportedly suffered significant infrastructure damage[14].

Factors in Software Supply Chain Vulnerabilities

Working to help ensure an organization's security against cyberattacks has always been a challenging undertaking. But what significantly complicates this situation is the added complexities in addressing potential risks associated with goods and services provided by supply chain partners. This is especially true when it comes to software and software components provided by third-parties.

Specific cybersecurity risk factors associated with the software supply chain include:

- *Dominance of third-party software*—As previously noted, organizations overwhelmingly depend on third-party software, software components and software code to control essential operations and for integration into finished products. Even companies that develop or operate proprietary software platforms often rely on component code from third-parties to speed development and increase dependability.

- *Growing number of third-party software and software component suppliers*—Increasingly, software supply chains are mimicking traditional supply chains in their length and in the number of participating suppliers. In addition, software as a service (SaaS) providers are gaining in importance, as more organizations are seeking to control infrastructure costs by moving critical IT systems to cloud-based alternatives.

- *Varying levels of software quality control*—The expanded use of third-party software and SaaS providers predictably leads to wide differences in the quality and security of available software products, components and services. The absence of standardized metrics for these characteristics means that organizations must rely on the assurances of software suppliers, or conduct their own independent evaluations.

- *Known and unknown software vulnerabilities*—According to one estimate, 97 percent of cybersecurity incidents can be traced back to the failure to patch vulnerabilities in existing software or software applications.[15] In software that includes multiple third-party components that risk can increase mathematically. Further, this level of risk does not account for vulnerabilities that can only be identified once software has been released and exposed to attack in actual use.

- *Counterfeit software*—The use of third-party software also introduces the risk of unknowingly downloading or using counterfeit versions of authenticated software or software components. Counterfeit software may contain malware that can access critical system data. And legitimate software suppliers routinely address known vulnerabilities by supplying patches that are not available to counterfeiters.

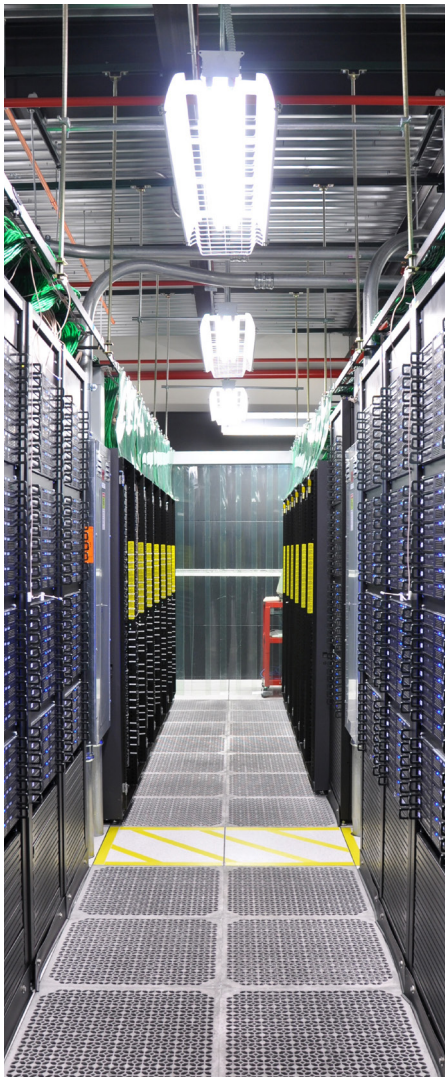
- *Inadequate vendor management and risk management practices*—Finally, many organizations fail to implement and maintain sufficiently robust vendor management and risk management programs and practices that can identify potential cybersecurity concerns for software and software components procured from third-parties, or which evaluate a supplier's ability to respond quickly to newly identified vulnerabilities.

For critical infrastructure organizations and entities, these and other risk factors heighten the importance of evaluating software supply chain vulnerabilities, and developing and implementing programs that can help reduce cybersecurity risks connected with third-party software.

Some Best Practices for Mitigating Software Supply Chain Risks

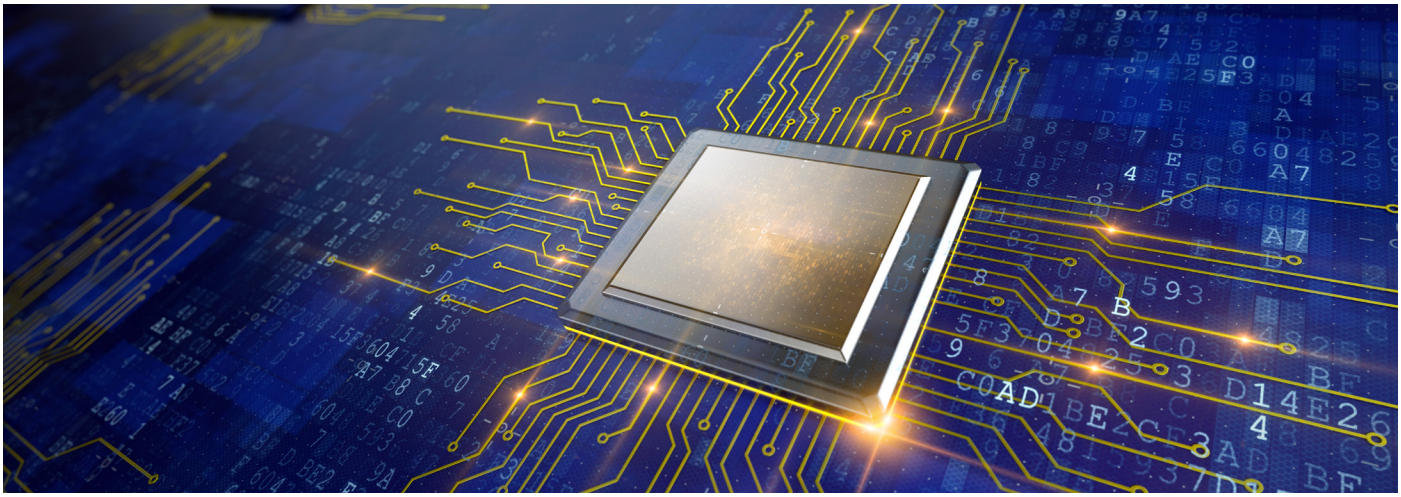
While every organization is different, there are some basic principles and best practices that are universally applicable and that can help mitigate cybersecurity risks introduced through software supply chain activities. At a minimum, an effective software supply chain management program should include the following elements:

- The development of formal security specifications and requirements for all third-party software products and components; inclusion of these specifications by reference in every request for proposal (RFP) and vendor agreement;
- A due diligence assessment of new software supply chain suppliers to determine whether adequate safeguards are in place to minimize cybersecurity risks associated with the use of their software or software components, with regular follow-up audits;
- A procurement policy that requires independent validation of third-party software for sufficient protection against security flaws and weaknesses for all software applications to identify potential vulnerabilities that may result in a security incident;
- A formal process for regularly updating software applications and applying patch releases as appropriate to help ensure continued protection against newly identified threats;
- Initial and periodic validation testing of software and software components for compliance with the organization's security specifications; wherever possible, testing should be automated to reduce risks associated with human intervention;
- Implementation of "track and trace" programs to establish and monitor the sources of all software, software



components and code, to facilitate efficient access to software updates and security patches and to help ensure ongoing support for legacy products;

- Limiting on a “need to know” basis access by individual software vendors to information about the organization’s overall software strategy or current or planned software systems;
- Clear software vendor policies with unequivocal consequences for non-compliance with mandated security specifications or the use of counterfeit software or software components; and
- Ongoing employee training to raise and maintain awareness of effective security practices regarding the software supply chain, the selection of third-party software and components and the monitoring of software systems for potential vulnerabilities.

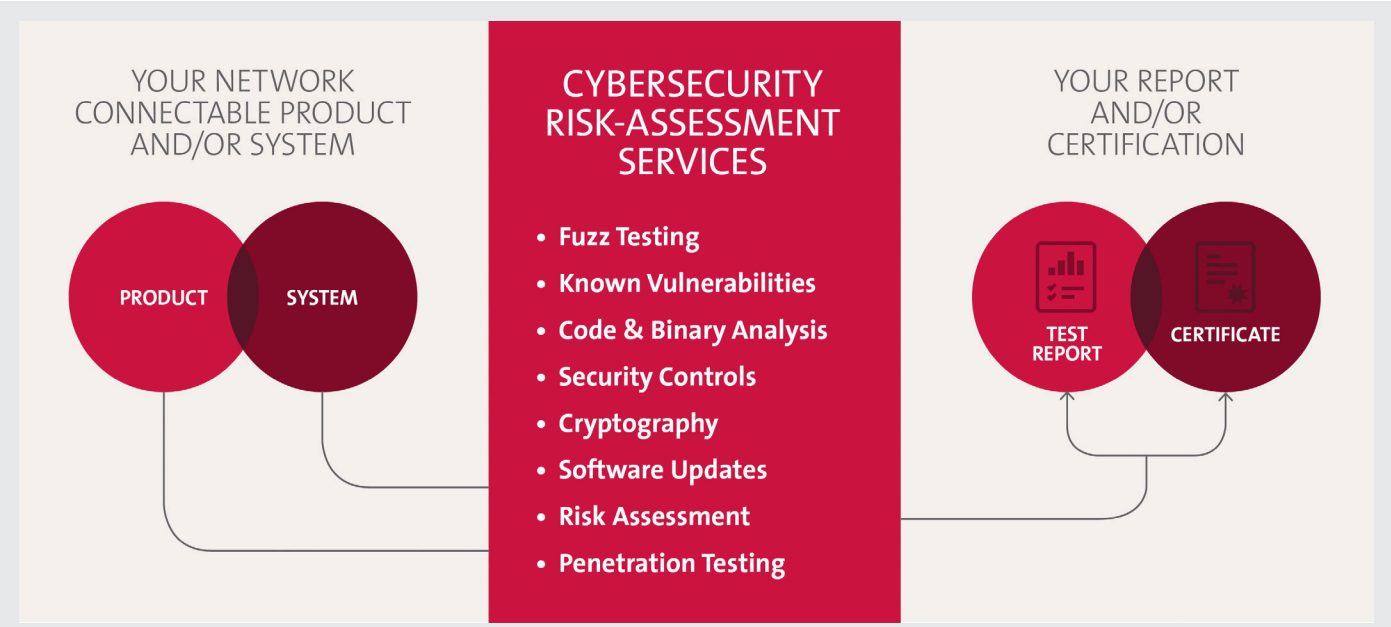


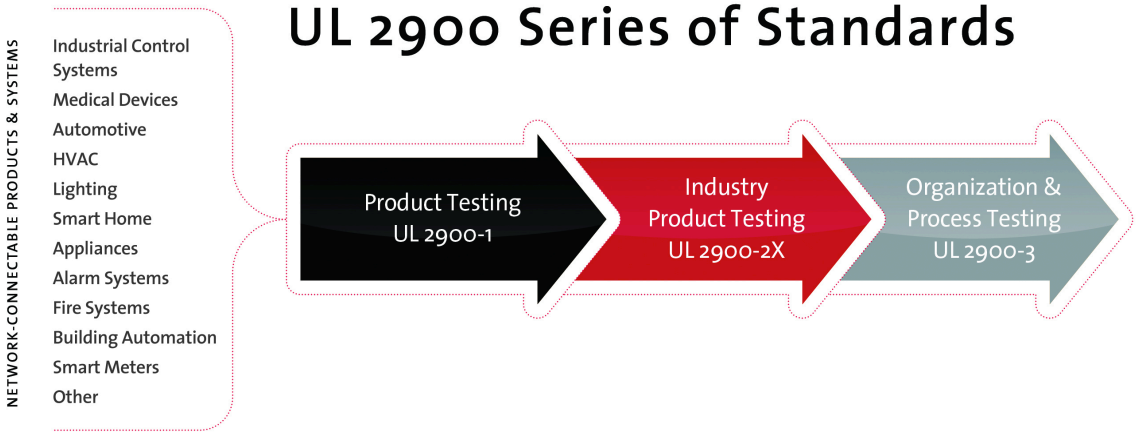
UL's Cybersecurity Assurance Program (CAP) and the UL 2900 Series of Standards

A number of standards are currently available to address key aspects of the safety and security of network-connectable products and systems. While these standards may be helpful in addressing overall potential vulnerability to cyber threats, they do not directly evaluate cyber threats associated with software. Further, these standards do not provide clear and objective criteria to assess the actual effectiveness of software design or features intended to thwart software-directed cyberattacks.

To address these gaps, UL has introduced its Cybersecurity Assurance Program (CAP). UL CAP represents a holistic approach to mitigating cybersecurity risks that evaluates both product-specific and systemic immunity to cyber threats. This approach can provide critical infrastructure organizations with greater assurances regarding the security of third-party software and components, thereby minimizing their vulnerability to cyberattacks and the potentially costly consequences.

At the heart of UL CAP is a series of UL Outlines of Investigations that provide verifiable criteria for assessing the cyber vulnerability of network-connectable products and systems. Specifically, the UL 2900 series, Standard for Software Cybersecurity of Network-Connectable Devices, is applicable to a broad range of interconnected devices and systems, and is intended to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase overall security awareness.





The UL 2900 series currently consists of standards in the following categories:

- *General Product Requirements*– Standards in this category include UL 2900-1, Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements. UL 2900-1 evaluates software for the presence of security risk controls in its architecture and design, using prescribed testing methods to evaluate vulnerabilities, software weakness and malware.

- *Industry Product Requirements*– At present, there are two standards in this category. They are UL 2900-2-1, Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems, and UL 2900-2-2, Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems. These standards evaluate vulnerabilities of software that supports devices and systems used in the specified industry environment. Additional standards in this category are currently under development.

- *General Process Requirements*– Currently under development is UL 2900-3, Outline of Investigation for Software Security of Network-Connectable Products, Part 3: General Requirements. This series of standards is expected to address the general testing of organizational systems and processes for conducting the risk assessment necessary to determine applicable, software-based cyber threats and the ability for teams to include security in the product development process.

Utilized together, the UL 2900 series of standards provides an effective framework within which to evaluate an organization's overall approach to software security as well as the specific vulnerabilities of individual third-party software and software components. As such, it provides critical infrastructure entities with the criteria necessary to measure and assess the security features of products, the technologies deployed and likelihood that weaknesses can be exploited.

Summary and Conclusion

The expanded use of third-party software and software components has contributed to the increase of software-based cyberattacks on critical infrastructure industries as well as other entities. Accordingly, it is vitally important for organizations to establish and maintain robust risk management strategies that can reduce its vulnerability to potential cyber threats originating from the software supply chain. Such strategies can help to reduce unplanned downtime of mission-critical operations, the loss or compromise of secure data and potential damage to other assets.

UL CAP and the UL 2900 series of standards are founded on UL's extensive experience in developing standards, systems and protocols for evaluating the safety and security of connected technologies. They can help mitigate cyber security risks by providing a framework within which critical infrastructure organizations can establish security criteria for third-party software and thoroughly validate security claims of software vendors. And UL CAP provides an effective approach for improving overall cyber hygiene across all supply chain activities.

For more information about UL CAP and the UL 2900 series of standards, visit **http://ul.com/cybersecurity**, or contact **ULCyber@ul.com**.

©2016 UL LLC. All rights reserved. This white paper may not be copied or distributed without permission. It is provided for general information purposes only and is not intended to convey legal or other professional advice.

Endnotes

[1] "Protecting the open source software supply chain," posted on GCN, 22 July 2016. Web. 25 July 2016. https://gcn.com/Articles/2016/07/22/software-supply-chain.aspx.

[2] "International CIIP Handbook 2008/2009," ETH Zurich, Center for Security Studies, July 2008. Web. 15 April 2016. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=91952.

[3] "ICS-CERT Fiscal Year 2015: Final Incident Response Statistics," ICS-CERT Monitor, published by the U.S. Department of Homeland Security, November/December 2015. Web. 8 August 2016. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.

[4] See "CIP Standard," website of NERC, the North American Electric Reliability Organization. Web. 8 August 2016. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[5] See "Chemical Facility Anti-Terrorism Standards Risk-Based Performance Standards Guidance," website of the U.S. Department of Homeland Security. Web. 8 August 2016. https://www.dhs.gov/publication/cfats-rbps-guidance.

[6] "Executive Order 13636—Improving Critical Infrastructure Cybersecurity," February 19, 2013. Web. 15 April 2016. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[7] "Framework for Improving Critical Infrastructure Cybersecurity," U.S. National Institute of Standards and Technology (NIST), February 12, 2014. Web. 15 April 2016. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[8] "US government hack stole fingerprints of 5.6 million federal employees," Associated Press, as published in The Guardian, 23 September 2015. Web. 8 August 2016. https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints.

[9] "Semi-Annual Report to Congress, October 1, 2014-March 31, 2015," U.S. Office of Personnel Management, Office of the Inspector General. Web. 8 August 2016. https://www.opm.gov/news/reports-publications/semi-annual-reports/sar52.pdf.

Endnotes

[10] "Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security, February 25, 2016. Web. 8 August 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[11] "At Experian, Security Attrition Amid Acquisitions," KrebsonSecurity blog posting, 8 October 2015. Web. 8 August 2016. http://krebsonsecurity.com/tag/experian-breach/.

[12] "Anthem: Hacked Database Included 78.8 Million People," The Wall Street Journal, February 24, 2015. Web. 8 August 2016. http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.

[13] "Anthem's stolen customer data not encrypted," c|net, February 6, 2015. Web. 8 August 2016. http://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/.

[14] "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," Wired Magazine, January 8, 2015. Web. 8 August 2016. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[15] "2016 Data Breach Investigation Report," Verizon, April 2016. Web. 8 August 2016. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.