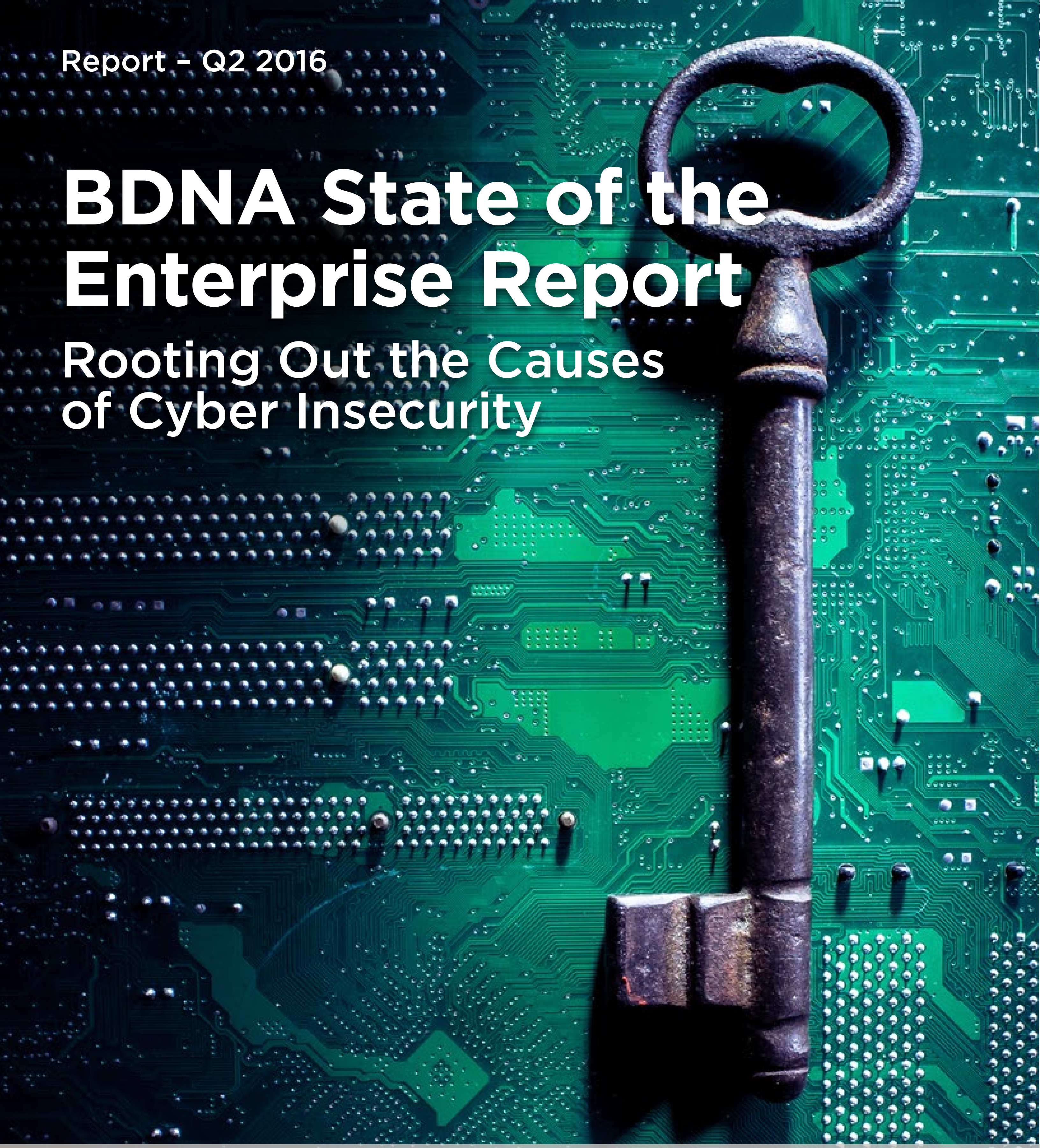
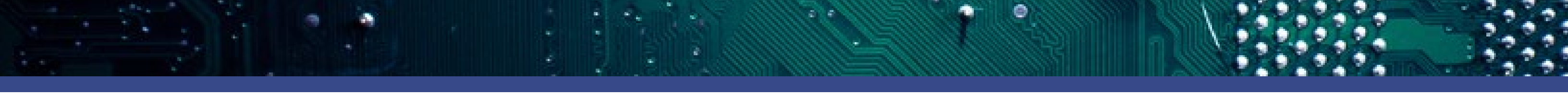
Report – Q2 2016

BDNA State of the Enterprise Report

Rooting Out the Causes of Cyber Insecurity



BDNA



The 2016 Cybersecurity Intelligence Landscape

The most widespread technology trends of the last decade – mobile devices, virtualization and cloud computing – combined with emerging trends, such as the Internet of Things, have vastly increased the potential attack surface of enterprise organizations for hackers and cybercriminals. While new technology has led to great gains in productivity, commerce and connectedness, it also has made us more exposed to cyberattacks, as evidenced by frequent headlines informing us of almost weekly enterprise data breaches affecting banks, retailers and government agencies.

If there is a silver lining to the growing number of cyberattacks, it is the increasing awareness among the public and within enterprises of where potential risks lie. This new knowledge of the hazards of phishing schemes, public networks and “Mickey Mouse” passwords has gone far toward protecting sensitive data from some of the most common threats.

Despite this progress, awareness still lags around one of the core vulnerabilities that typically plagues almost all corporate and government networks: the existence of out-of-date software and hardware assets that sit unprotected, living unnoticed within otherwise vigilant enterprises.

Addressing a Root Cause of Cyber Vulnerabilities: End-of-Life Assets

One of the most fundamental challenges that thwarts effective cybersecurity in enterprises and government agencies is the failure to track all IT assets on their networks. The most notorious and harmful breaches in recent years – “Heartbleed” and “Shellshock” among them – were possible not because of credit card skimmers or password phishers, but because of known software flaws left unprotected in assets that had passed their end-of-life (EOL) dates.

Once a piece of software or hardware has passed its end-of-life cycle, it is no longer maintained or supported by its originating vendor. That means the asset’s vendor no longer proactively monitors or issues patches for cyber vulnerabilities that can be exploited by hackers. So any vulnerabilities that do exist can serve as a gateway into the network that the software is installed on. Even the most common operating systems eventually reach their end-of-life dates, as millions of Windows users who must migrate to Windows 10 are well-aware.

Anecdotal evidence finds that between 30 to 50 percent of hardware and software assets installed in the average large enterprise are past their EOL dates. In the wake of a 2013 breach of an outdated version of Adobe ColdFusion software that compromised 53,000 current and former Department of Energy (DOE) employees’ personal information, the agency found that 40 percent of its software assets were beyond their EOL dates.

"We had a cybersecurity breach [in 2013] and one of the weak points was … out-of-date software," Rick Lauderdale, chief architect, Office of the CIO, Department of Energy, told Government Computer News.

The breach prompted DOE to develop a better record of information for its IT assets. After implementing a new IT asset management strategy that included solutions to identify and prioritize the most high-risk EOL assets, the agency was quickly able to reduce the EOL percentage of its software assets from 40 percent to 18 percent, and put a plan in place to work toward completely eliminating all EOL assets.

Another challenge today's enterprises face is the proliferation of unapproved hardware and software that employees install without approval. These unknown assets represent potential unchecked vulnerabilities that undermine security, data governance and efficiency.

The core problem concerning noncompliant and out-of-date assets is that IT teams lack awareness of them. A 2016 Ventana Research report, "Establishing Cybersecurity Intelligence: Identifying Risk and Vulnerability in IT Assets," found that less than one-quarter (only 24 percent) of organizations say it is "easy" or "very easy" to access and use data to measure and assess risk. Depending on the size of the organization, there could be thousands of separate software titles installed at any one time, with versions labeled numerous different ways – far too many to be easily tracked and monitored for vendor support status or end-of-life horizons.

"The least recognized yet potentially greatest risk to your operation is a security breach of your IT assets," according to the Ventana Research report. "Every piece of hardware and version of software that is not maintained regularly could be a gateway for unauthorized access. What's needed is cybersecurity intelligence, a new discipline designed to protect IT assets from attacks."

The key challenge enterprises face in this regard is to improve their IT visibility from a cyber perspective so they are continuously aware of what is on their networks and what the cybersecurity properties (including EOL data) of those assets are. To do this, organizations must proactively augment and normalize IT data from their IT assets residing in their traditional IT inventory applications, whether that might be Microsoft System Center Configuration Manager (SCCM), ServiceNow Discovery, VMware vCenter Protect, Tanium, IBM Tivoli Asset Discovery, HPE Universal Discovery, BMC Discovery or Altiris Client Management, among many others.

4 Steps to Protect Your Asset Inventory

1. For a complete view of potential risks, acquire a comprehensive catalog from a third party that provides details on vendors, products, release dates and other details. Using one can reduce the time, resources and cost needed to manage IT assets.

2. Match your technology asset inventory to it, and ensure your catalog is always up-to-date to support the analysis and actions that are required.

3. Compare your inventory and industry catalog with vendor-supplied version information to identify outdated technology and the greatest risks to the organization.

4. Take action on immediate threats that could impact the security of IT assets and the information they contain.

Source: 2016 Ventana Research, "Establishing Cybersecurity Intelligence: Identifying Risk and Vulnerability in IT Assets

Once that IT asset data is augmented and normalized, it must be fed to downstream third-party tools — such as information technology service management (ITSM), governance, risk and compliance (GRC), and cybersecurity applications from vendors such as ServiceNow, RSA Archer, HPE Asset Manager, Troux by Planview, and Apptio Platform — to ensure that data is acted upon to mitigate risk. This enables a proactive prioritization of mission-critical assets, propelling a continuous risk management cycle.

This approach of building continuous awareness, monitoring, and mitigation of IT vulnerabilities is a core tenet of the Risk Management Framework (RMF), created by the National Institutes of Standards and Technology to help commercial and governmental organizations build methodical and systematic approaches and processes to improve their cyber risk management.

Automation as Key to the Future of Cybersecurity

Today's modern corporate and government IT environments are more complex than ever, relying increasingly on mobile devices, virtual hardware and software, and applications that attach easily to the network. Managing and proactively protecting IT assets in this new environment presents a mounting challenge – the sheer volume of items to be cataloged and tracked is more than can reasonably be done manually.

For this reason, establishing an automated process for discovering and categorizing IT asset inventories is a crucial step that must be taken to identify what exists in a given enterprise — after all, you can't manage and protect what you can't see. With automation, the discovery process that would have required untold time and resources to tackle manually can be completed in hours or days, and can be continually updated as assets are added to or removed from the network. Once all assets are visible and accounted for, they can then be tracked against crucial characteristics, including EOL dates, compliance with IT policies and vendor licensing requirements.

The greatest benefit of having complete visibility of all IT assets — coupled with product and market intelligence — comes from how IT leaders can then leverage the new insights and knowledge to help address their organization's priorities and act quickly to fix and remediate the most pressing vulnerabilities created by unpatched and uncompliant assets. This capability also enables proactive decision making on technology modernization priorities.

Furthermore, data shows that taking action to address vulnerabilities as they are identified is an almost guaranteed way to prevent an attack. According to the Verizon 2015 Data Breach Investigations Report, a shocking 99.9 percent of all exploited vulnerabilities occurred more than one year after the vulnerability was first identified.

If asset cybersecurity is done effectively, it will save enterprises money and potential damage to their brand and reputation. If neglected, they will, over time, add substantial costs for any enterprise.

About BDNA

BDNA® creates the most authoritative enterprise technology data. Armed with this invaluable information, enterprises will make the best decisions possible, lower costs and risks as well as accelerate the pace of their business. To produce the most relevant results, BDNA maintains Technopedia®, the most complete, current and reliable content repository about hardware, software and medical devices. This catalog is the foundation from which BDNA creates the highest quality enterprise technology data in the industry, which in turn results in visibility, insight and information enterprises can trust. Venture-backed and based in Mountain View, Calif., BDNA operates globally with customers across all segments and vertical markets. For more information, please visit **www.bdna.com**.