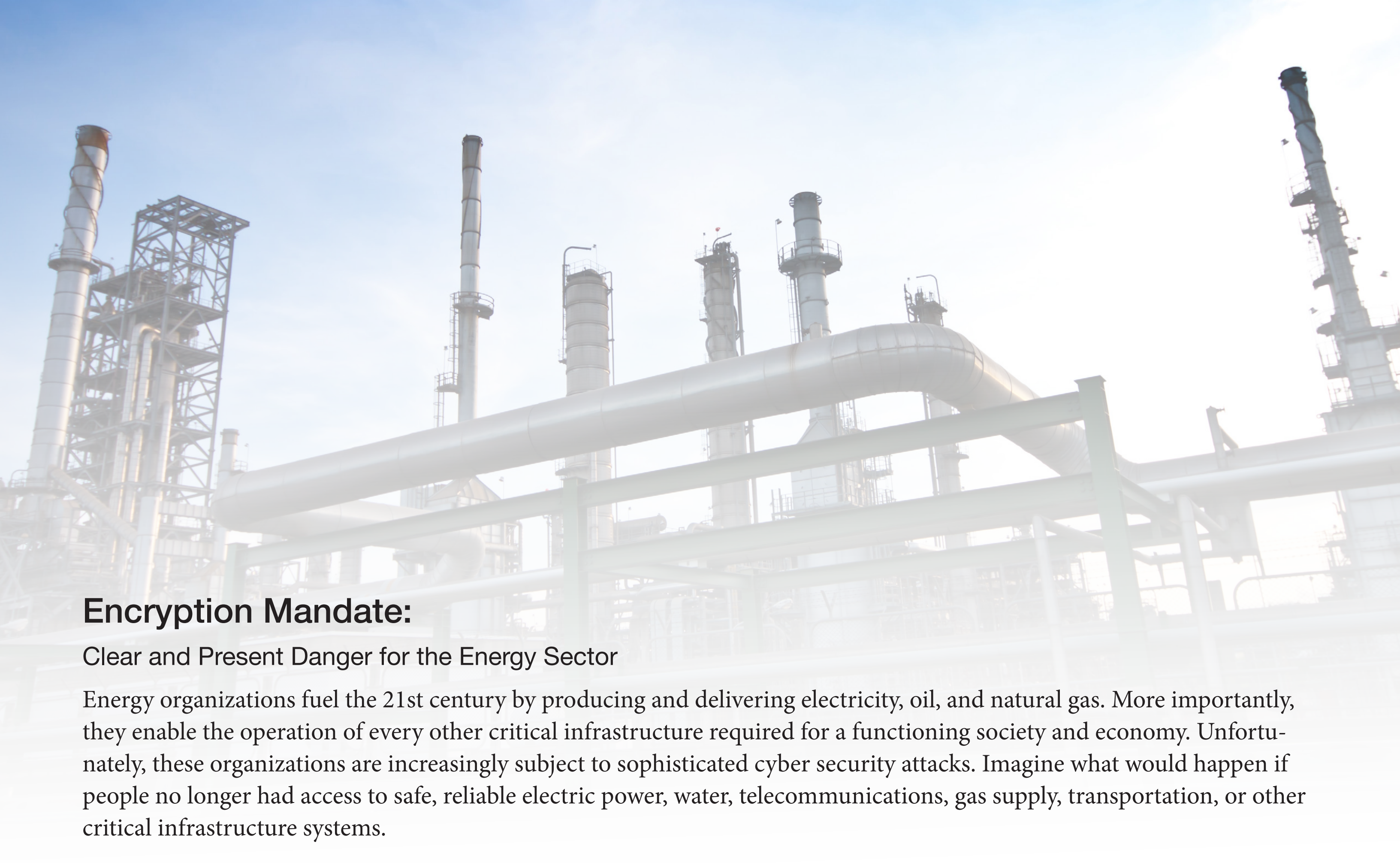

Encryption Mandate:

Clear and Present Danger for the Energy Sector

Energy organizations fuel the 21st century by producing and delivering electricity, oil, and natural gas. More importantly, they enable the operation of every other critical infrastructure required for a functioning society and economy. Unfortunately, these organizations are increasingly subject to sophisticated cyber security attacks. Imagine what would happen if people no longer had access to safe, reliable electric power, water, telecommunications, gas supply, transportation, or other critical infrastructure systems.

Critical Industrial Control Systems (ICS) are at risk

Industrial Control Systems (ICS) (including Supervisory Control and Data Acquisition (SCADA) systems) monitor and control the physical equipment and processes used by oil, gas, electricity, and utility companies. Unlike typical computers and operating systems, the majority of embedded devices used in ICS systems are five to ten years old and are infrequently updated. Worse, they have little or no native security designed into them because they were never intended to be operated remotely over the Internet.

Despite these concerns, ICS systems are increasingly connected to multiple, external networks and the Internet where they share real-time generation, transmission, and distribution data with regional load-balancing entities, marketing partners, trading teams, and other departments. What's more, these systems are frequently administered remotely using handheld mobile devices owned by system administrators that are outside of the energy company's control. It's no surprise that ICS and SCADA systems represent an extremely attractive target for those with malicious intentions.

In June of 2015, the SANS Institute released survey results from energy professionals who actively operate or support industrial control systems. The report found that:

- 32% indicated their control system assets or networks had been infiltrated or infected at some point
- 34% believed their systems had been breached more than twice in the past 12 months
- 17% acknowledged six or more breaches during 2015 (up from 9% from 2014)
- 15% reported needing longer than a month to detect a breach
- 44% were unable to identify the source of the infiltration

A recent FireEye threat intelligence report shows that while 75% of respondents feel that their organization is a target for an attack that could cause physical damage only 35% have the ability to track actively all of the threats confronting their networks. Likewise, a Tripwire survey found that 69% of oil and gas companies are not confident their organization can detect all cyberattacks.

Energy-specific Cyberattacks are increasing and causing significant damage

As the number of Internet-facing embedded devices and control systems rises, the number of attacks targeting ICS systems (particularly energy-generation systems) is likewise increasing – and so is the risk. Just consider the 2015 BlackEnergy attack on a Ukrainian power plant that left over 700,000 customers without electricity.

A different 2016 Study by Tripwire shows that energy, utilities, and oil and gas organizations are experiencing a disproportionately large increase in cyberattacks when compared to other industries over the last 12 months. In addition, more than 68% of respondents said that the rate of successful cyberattacks had increased by over 20% in the last month alone. Likewise, a 2015 U.S. Department of Homeland Security report shows that critical infrastructure attacks are on the rise and that the energy sector faces more cyberattacks than any other industry. The report states that in 2014, Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents. Of these, 79 (32%) were in the energy sector, and 55% involved advanced persistent threats or sophisticated actors. At first glance, the total number of attacks may seem small compared to cyber incidents in other industries: however, according to ICS-CERT, many more energy sector incidents go unreported or worse, undetected.

Both public and private energy organizations are facing increasing attacks on a global basis. Consider the famous Stuxnet case: a computer worm was delivered into Iran's Natanz nuclear fuel enrichment facilities(through a worker's thumb drive) where it reportedly destroyed roughly 20% of Iran's nuclear centrifuges by causing them to spin out of control. Other attacks including "Dragonfly" (as named by Symantec) or "Havex" (as named by F-Secure) implemented a remote access Trojan horse program (or RAT), which enabled unauthorized persons to monitor, disrupt, and even sabotage wind turbines, gas pipelines, and power plants quickly and remotely. It also downloaded and installed other malicious software that successfully targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

Encryption and Security in Brief

Before learning how to protect data, it's useful to know a little more about the data itself — specifically where it resides. For our purposes, data exists in the following three "states": at rest, in transit, and in use. Data at rest refers to data located in persistent storage, such as a hard drive. This could be as simple as a saved document or image. Data in transit is any data sent or received across a network. Downloading a file from the Internet or transferring a file between two computers on a local area network are both cases of data in transit. Data in use is a little trickier, but it essentially means any data that a computer's CPU is actively processing or data temporarily stored within a system's RAM.

Encryption is a deep, complicated subject that many experts devote their lives to mastering, but having a rudimentary grasp of the key terms and concepts will help healthcare organizations better understand what it takes to be compliant. Ideally, sensitive data should be secure enough that unauthorized parties can't even access or obtain it. Even if data falls into their hands, though, they definitely shouldn't be able to read it. That's where encryption comes in.

Encryption transforms data to make it unreadable without authorized access. In this case, authorized access comes in the form of a decryption key, which is fairly self-explanatory. When the right people have the key, they can read your encrypted data; the wrong people who don't have the key cannot.

Many encryption methods exist, as do different instances when encryption is necessary. Encrypting data stored on a hard drive is one example, while accessing a business's network remotely over a virtual private network is another. Unfortunately, when it comes to compliance, there's no universal standard for encrypting data. The regulations that govern how each industry handles data may not dictate the same encryption requirements.

People with a passing familiarity with encryption may have heard of 128-bit, 192-bit, or 256-bit encryption. This refers to the "size" of the key, in bits, necessary to decrypt data. A 128-bit key corresponds to a total of 2128 possible keys; a 256-bit key represents 2256 possibilities. Generally, a larger key requires more time to crack via brute force methods (where an attacker uses a computer, or multiple computers, to "guess" the key). Security experts agree that it would take modern computers billions of years to brute-force a 128-bit key. Radical advancements in computing technology (quantum computing, for example) would be necessary to break 256-bit encryption.

Of all the encryption methods, AES (Advanced Encryption Standard) receives the lion's share of attention, and for good reason. The NSA uses AES to encrypt data, which ought to be proof enough of its security. AES can use 128-bit, 192-bit, or 256-bit keys and thus far has been extremely resistant to attempts at exploiting potential weaknesses. Several cryptographers have tried to break AES, but none have succeeded.

If there's a downside to AES, it would be in the computational cost of its operation. For many years, most digital encryption on computers was performed "in software," where the systems CPU performed all of the necessary encrypt/decrypt operations. This work proved exceptionally cumbersome for general purpose processors and could bring a lower-end system to its knees. Only relatively recently have Intel's AES New Instructions (AES-NI) and other innovations integrated specific encryption acceleration silicon into CPUs (thus running "in hardware") and made the burden of encryption computation negligible. This also applies to the encryption of external drives, including flash drives. Somewhere, a component crunch those encryption processes, and if there's no dedicated acceleration behind the work, other applications running on the system may suffer.

In addition to protecting data via encryption, it's important to authenticate both data and communications (i.e., transmitted files and messages) to ensure that the data received matches the data sent. Verifying data arrived from true and trusted sources is another key aspect of maintaining security, which is why security professionals recommend cryptographic hashing. A hash is a number produced from a string of text that acts like a digital fingerprint. When someone sends a message, for example, they can generate a hash and include it with the message. The recipient of the message can then create a hash of the received message and compare it with the original hash. If the two match, the message's authenticity is confirmed. Spoofing a hash is virtually impossible, so this tactic offers one way to ensure files and messages weren't tampered with.

Encryption can — and should — happen in a variety of ways in a variety of situations. Windows BitLocker drive encryption is an example of one essentially free solution in the consumer space. Other times, certain hardware may be handy for encrypting data without the need for separate software. Such "self-encrypting" hardware options exist for large hard drives as well as portable flash drives. Web traffic can be encrypted using SSL (Secure Socket Layer), and the list goes on. Simply put, if desired, diligent users can keep their data encrypted wherever it goes.

Many Types of Sensitive Information Must Be Protected

In addition to attacks targeting ICS systems, energy organizations must protect sensitive data ranging from intellectual property to trade secrets to financially valuable data, such as quarterly or annual reports. They must also protect employee and customer personally identifiable information (PII) and even credit card and banking information such as addresses, date of birth, social security numbers, and account numbers.

U.S. Energy companies have been attacked and had proprietary data files stolen and sent overseas in foreign attempts to acquire technical diagrams, schematics, and valuable "bid data" detailing the quantity, value, and location of oil discoveries worldwide. Operation Night Dragon (named by McAfee) was one such cyberattack designed to steal sensitive data from energy companies.

In 2013, online attackers successfully penetrated the Department of Energy (DOE) network and targeted employees' personal data, rather than top secret energy or nuclear information. Attackers obtained personally identifiable information (PII) pertaining to several hundred of the agency's employees and contractors. In response, a DOE memo urged all employees "to help minimize impacts and reduce any potential risks" by encrypting all files and emails that contained PII, regardless of where stored, be it on hard drives, removable media, or on a shared network."

Security Breaches Are Expensive

Data theft can result in not only immense damage to critical infrastructures – disrupting the daily lives of millions of people – it can also cripple an energy company through unauthorized access to monetary operations, loss of intellectual property, disclosure of merger-and-acquisition deals, identity theft, and the loss of personally identifiable information of employees and customers. This types of theft can result in loss of competitive advantage in accessing new fields, failure to keep current clients and investors, regulatory fines, liability lawsuits, share price drops, and other reparation expenses – all of which can damage a firm's reputation and financial standing, not to mention cause an adverse ripple effect across third-party partners throughout the industry.

In 2016 the average cost of a data breach in the U.S. was $7.01 million per incident or on average, $221 per lost or stolen record, and these costs are even higher for energy organizations. According to the Ponemon Institute, the expense of data breaches varies by industry and energy organizations have higher than average costs at $246 per lost or stolen record. These potential expenses equate to over $7.3 million for each incident that impacts an energy organization (using Ponemon's average number of breached records per incident of 29,611) and many organizations experience more than one data breach.

Complex Regulatory Environment Adds to Security Burden

In addition to facing evolving risks from cyber security threats and an aging infrastructure, the energy sector is also subject to highly complex regulations in various forms that are often overseen by numerous jurisdictions, which makes it arguably the most difficult of industries to protect and secure.

Control System Security Standards

According to data from the 2015 SANs Institute survey “The State of Security in Control Systems Today,” the top five energy security standards in use in the United States are:

1. U. S. National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82r2) — Provides guidance for establishing secure industrial control systems (ICS).
2. North American Electric Reliability Corporation Critical Infrastructure Protection standards (NERC CIP) — Outlines how to identify and protect critical cyber assets for organizations that deliver bulk electricity to the North American electrical power grid.
3. Center for Internet Security’s (CIS) Critical Security Controls v6.0 — Recommends a set of actions for cyber defense that provide specific and actionable ways to stop today’s most pervasive and dangerous attacks
4. ISA99 Industrial Automation and Control Systems Security (IEC 62443) — Develops and establishes standards, technical reports, and related information that defines procedures for implementing electronically secure industrial automation and control systems and security practices and assessments of electronic security performance.
5. ISO 2700 Series (including 27001 and others) — Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

Additional energy security standards may include:

- ENISA Guide to Protecting ICS (recommendations for Europe and Member States)
- ISA100.15 Backhaul Network Architecture for wireless manufacturing and control systems
- Qatar ICS Security Standard
- U.S. Department of Homeland Security’s Chemical Facility Antiterrorism Standards (CFATS)

NIST Guide to Industrial Control Systems (ICS) Security

The NIST Guide to ICS Security Special Publication 800-82r2 provides guidance for establishing secure industrial control systems (ICS) including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC). The document offers an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Special Publication 800-83r2 is part of the NIST Special Publication 800 series of documents on information technology published by the NIST Information Technology Laboratory (ITL), which focuses on research, guidance, and outreach efforts in computer security across industry, government, and academic organizations. Security topics include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management.

NERC CIP

The Federal Energy Regulatory Commission (FERC) oversees the power industry but gives the North American Electric Reliability Corporation (NERC) the responsibility for maintaining and complying with Critical Infrastructure Protection (CIP) standards. NERC CIP requires organizations that deliver bulk electricity to the North American electrical power grid to define methods, processes, and procedures for securing critical cyber assets, as well as the non-critical cyber assets within the electronic security perimeter. (“Cyber assets” are loosely defined as all “programmable electronic devices and communication networks including hardware, software, and data.”) Penalties for non-compliance with NERC CIP can include fines, sanctions, and/or other actions against covered entities. Because NERC is a trans-national organization, the exact penalties vary from country to country.

Center for Internet Security Critical Security Controls (CIS) v6.0

The Center for Internet Security's Critical Security Controls version 6.0 recommends a set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principle benefit of the Controls is that they prioritize and focus on a smaller number of actions with high pay-off results. Created by the people who know how attacks work (e.g. NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations, and some of the nation's top forensics and incident response organizations), the Critical Security Controls help answer the question, "what do we need to do to stop known attacks."

The Controls are derived from the most common attack patterns and are updated by cyber experts using actual attack data pulled from a variety of public and private threat sources. They are then vetted across a very broad community of government and industry practitioners to create actionable guidance to improve individual and collective security in cyberspace. The Controls are also updated based on new attacks as they emerge.

ISA99 Industrial Automation and Control Systems Security (IEC 62443)

The ISA99 standards development committee brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security. The ISA99 Industrial Automation and Control Systems Security (IEC 62443) is a set of standards, technical reports, and related information that define procedures for implementing electronically secure industrial automation, control systems, security practices, and assessment of electronic security performance. It is designed for users, system integrators, security practitioners, and control systems manufacturers and vendors who design, implement, or manage industrial automation and control systems. Compliance with ISA99's guidance is intended to improve system electronic security and help identify and address vulnerabilities. This, in turn, reduces the risk of compromising confidential information or causing degradation or failure of the process equipment under control.

ISO 2700 Series

A relatively new organization, the ISO 2700.org is an alliance of information security consultants from across the world. The ISO 2700 standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization. The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

Data Security Standards

Depending on the type of organization, energy companies may also be subject to compliance regulations intended to secure financial information for public companies and personally-identifiable (PII) data. These regulations include:

1. Sarbanes-Oxley Act of 2002 (SOX) – Focuses on improving corporate governance and enhancing the accuracy and security of financial reporting.
2. The International Traffic in Arms Regulations (ITAR) regulations — Oversees the safe export and temporary import of defense articles and services. It is governed by 22 U.S.C. 2778 of the Arms Export Control Act (AECA) through the U.S. Department of State.
3. The Payment Card Industry Data Security Standard (PCI DSS) — Impacts an organization's payment systems and applies to organizations which use third-party vendors to process credit card transactions.
4. Various state data breach notification laws — Requires organizations to notify individuals of security breaches of information involving personally identifiable information, such as California's S. B. 1394.

Real Risk

Today, encryption is a staple of the professional world. Virtually every industry that deals with personal and/or sensitive data relies on encryption to protect that data. Energy organizations that don't encrypt sensitive data put themselves at risk for stiff government penalties, fines, lawsuits, and more. Vendors that do business with them are also targeted for malicious data breaches.

The first step to avoiding these expensive, potentially crippling fines and other expenses associated with a breach is to pursue regulatory compliance. Regulatory compliance entails much more than simply password-protecting an office's workstations. It requires using encryption to protect data-at-rest when stored on computer systems or removable media devices. Indeed, data at rest that is outside the organization's firewall is the top source of security breaches. According to a Ponemon's 2015 study, 96% of respondents reported a security incident involving a lost or stolen device. Energy organizations and associated third-party vendors must safely store data to meet compliance requirements.

Chasing Compliance: How Regulations and Encryption Fit Together

Encryption is terrific…in theory. Data stays protected, and confidential information remains locked away from the wrong eyes. In reality, though, compliance costs money, whether from purchasing hardware and software, hiring a consultant, both, or possibly more. In some instances, a particular regulation will mandate encryption in clear, unmistakable terms; failure to comply with these terms implies a violation of the law. Other times, rules may be vague about encryption requirements, leaving a gray area for organizations to decipher. For example, a regulation may dictate protection for sensitive and/or personal data without explicitly stipulating protection via encryption. Obviously, these situations are less than ideal.

When the law isn't straightforward, security experts can provide clarity if and when a consensus gives way to commonly accepted best practices. The term isn't exclusive to regulations and encryption, but it can nonetheless help guide energy organizations that encounter nebulous compliance verbiage. Following industry best practices will keep organizations protected in times when the letter of the law proves hard to decipher. Sometimes even the government will come to an organization's aid with published best practices guidance, although the availability of such documents within a given niche or application can vary widely.

The Human Factor

Energy organizations can reasonably protect themselves against known threats. For instance, they can set up firewalls to thwart incoming attacks and use virtual private networks (VPNs) and secure communication protocols, such as HTTPS, to keep data secure while in transit. However, in many cases, an entity's weakest link is its employees.

In fact, the 2015 Ponemon study indicates that respondents worry more about employee negligence (51%) than any other security threat. That's ahead of cyber attackers (35%), system failures (19%), and identity thieves (a mere 5%). Note that negligent employees aren't the same as disgruntled types, which the report classifies as "malicious insiders." Only 19% of respondents listed these employees as a chief concern.

The biggest threat is well-meaning but inattentive employees. They're the reason laptops containing treasure troves of data disappear. Since accidents and theft do happen with all too frequent predictability, responsible enterprises maybe playing Russian roulette by not taking appropriate precautions: Ponemon's 2010 paper "The Billion Dollar Lost Laptop Problem" pegs the number at 7.12% across all surveyed organizations. Equipping portable devices with self-encrypting drives is one obvious step, but energy organizations should go further, particularly with at-rest data on removable storage. One might assume that a portable hard drive or USB flash drive will never be left unattended, but that's precisely the kind of employee wishful thinking and negligence that leads to breaches. Energy organizations must address this potential weakness.

Encrypt Data to Protect Critical Energy Infrastructure and Sensitive Information

Cybercrime is rising, and energy organizations are high profile targets. To protect against foreign or local espionage, disruptions to critical infrastructures, and to avoid data theft and misappropriation, energy organizations must take adequate security measures. Conducting a thorough security assessment and implementing data encryption are two immediate steps that organizations can take to avoid costly data breaches and safeguard critical infrastructure operation.

SOURCES

http://www.efile.com/efile-tax-return-direct-deposit-statistics/

https://www.ssa.gov/oact/STATS/OASDIbenies.html

http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

http://www.csoonline.com/article/2135661/identity-management/do-states-need-fisma-compliance--it-depends---part-2-of-2-.html

http://searchsecurity.techtarget.com/USB-thumb-drive-security-best-practices-spelled-out-by-NIST