Importance of Maintaining Effective Cybersecurity in Government Offices and Agencies

Cybercrime costs could hit $6 trillion annually by 2021; may potentially double during the coronavirus outbreak period.

— Cybersecurity Ventures, May 19, 2020

Organizations within the public sector encompass different functions including law enforcement, first responders, utility management, as well as state and city municipalities to name a few. All share a universal responsibility to maintain the security and sanctity of sensitive public information residing within their environments. Whether it be personal identification details, social security information, financial, health or criminal records, government entities hold a treasure trove of vulnerable public information which, if in the wrong hands, can lead to serious loss in reputation and public trust.

16% of security breaches in 2019 were in the public sector.
— "2020 Data Breach Investigations Report," Verizon

While often lacking in funding and necessary talent, government IT and security teams are required to maintain visibility across their fleet, ensure appropriate security controls are enforced, and adhere to data privacy regulations such as CJIS or HIPAA or adopt cybersecurity frameworks such as the NIST CSF. Without measures in place, unmonitored and vulnerable endpoints are often exploited by malicious intruders to gain privileged access to the corporate network to initiate large-scale attacks. The multitude of security breaches through phishing, malware intrusion, and ransomware coupled with the sudden rise in off-network devices due to the coronavirus outbreak, has organizations requiring security tools ingrained in automation and endpoint resilience to better set and enforce security policies.

GOVERNMENT'S IT AND SECURITY CHALLENGES

- Limited resources and talent to address cybersecurity gaps
- Safety and integrity of sensitive data to ensure public trust
- Increasingly remote, off-network device environment as a result of the coronavirus outbreak
- Compliance with data regulations such as CJIS or HIPAA
- Adoption of recommended cybersecurity frameworks such as NIST CSF
- Inability to track progress towards compliance based on reliable metrics
- Hardware and software inefficiencies brought up by legacy infrastructure

Average ransom demands are nearly half a million dollars, with total monetary value reaching into the millions.

— "2020 State and Local Government Security Report," BlueVoyant

Read more about Absolute's findings in endpoint security in the 2021 Endpoint Risk Report:

GET THE REPORT

STRENGTHEN SECURITY AND COMPLIANCE THROUGH ENDPOINT RESILIENCE

Absolute enables IT and Security teams to maintain visibility across their fleet, identify and protect sensitive information to better comply with data privacy regulations, and ensure their security gold image encompassing controls and applications remain intact across devices.

70% of breaches originate at the endpoint
— **IDC**

Enhanced Device Visibility

Absolute's Persistence technology, embedded in the firmware of devices at the factory, maintains visibility to the endpoint irrespective of whether it's on or off the corporate network as well as in the event of a hard drive swap or OS reimage. You can't secure what you can't see and so this unbreakable digital tether to the device is crucial to enforce security controls, especially in this post-pandemic environment of increased remote work.

Source of Truth Asset Intelligence

Absolute's unbreakable tether to the firmware ensures telemetry collected off the endpoint is always reliable and up to date. View a plethora of device metrics related to hardware and software details, device usage, and geolocation to monitor device activity and reduce inventory waste. Additionally, be alerted to hardware, software changes and set geofences to effectively respond to non-compliant events.

60% of data breaches in 2019 were linked to a vulnerability with a patch available but not applied.
— **"Cost and Consequences of Gaps in Vulnerability Response," ServiceNow, 2019**

Automated Endpoint Resilience

The first line of defense on the device is ensuring critical security controls remain active at all times. Absolute monitors and remediates the health of mission critical tools such as Anti-Malware, Encryption and VPN to maintain your fleet's security posture. Automatically run queries on or take action across multiple devices through custom or pre-built scripts to capture device parameters and respond to vulnerabilities that may arise.

Sensitive Data Discovery

Seamlessly search for sensitive corporate and public information residing across your fleet such as social security details, credit card numbers, criminal or health records to identify devices with the most at-risk data. Consequently, securely delete specific files or run a device wipe with confirmation to better comply with applicable regulations and prepare for internal or external audits with confidence.

164.7M sensitive records exposed in 2019.
— **Identity and Theft Resource Center**

Quarantine and Recover Missing Devices

Flag endpoints whenever they go missing and run a device freeze to render them inoperable to protect their residing data from potential cybercriminals. Then, leverage Absolute's Investigations team to recover the device for you. The team partners with law enforcement and uses your device's built-in digital tether along with forensics tools to track down its location, secure its data, attempt to identify an illegitimate user, and recover the device on your behalf.

ABOUT ABSOLUTE

Absolute is the leader in Endpoint Resilience™ solutions and the industry's only undeletable defense platform, embedded in over a half-billion devices. Enabling a permanent digital tether between the endpoint and the enterprise who distributed it, Absolute empowers IT and Security organizations with complete visibility, control, and Self-Healing Endpoint® security.

EMAIL: sales@absolute.com

WEBSITE: absolute.com

SALES: absolute.com/request-a-demo