Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

SEPTEMBER 2019

CONTROL OVER PRIVACY: SURVEY SHOWS A DISCONNECT BETWEEN CONSUMERS AND BUSINESSES

The 2019 Privitar Privacy Pulse survey of 5,128 consumer respondents and 751 business respondents in the U.S., United Kingdom, and France showed that consumers want more privacy control and businesses are working toward meeting consumer demands and putting data to good use.

Privacy Control

81%
of consumers need more control over the sharing of their personal data

VERSUS

79%
of the businesses feel they empower their customers to decide how their data is used and adequately explain this process

U.S. Consumers Looking for Enhanced Regulations

68%
of U.S. consumers agreed that stricter data regulations make them feel safer

Businesses: Risk/Reward of Taking Advantage of Data Opportunities

73%
of businesses feel they can enhance effective protection and management of their data

MEANWHILE

74%
of businesses feel they can do more to make their data accessible to the people who need it

BUT

66%
of businesses view the risks associated with using their data as not worth the benefits

---

Steps to Protect Data, While Gaining Insights

Privitar CEO Jason du Preez explained that organizations can take practical steps to address consumer trust and transparency issues, while also making the most of data to the point that data privacy becomes a competitive advantage.

- Be transparent by explaining when, how, and why consumer data is collected,
- Communicate data collection advantages to consumers—not just for them as individuals, but also for their communities,
- Establish data privacy teams, products, and governance, empower teams to set the best possible infrastructure that consistently adheres to regulations.

Source: Trust is at a tipping point: Consumers will react strongly if they feel their privacy is compromised, Help Net Security, May 6, 2019. https://www.esecurityplanet.com/threats/threat-hunting.html.

(continued)

WHAT IS THREAT HUNTING?

Advanced persistent threats are prolonged cyberattacks in which intruders gain unauthorized access to networks and remain undetected for an extended period of time. Typically, the intent is to monitor network activity and steal data. To combat advanced persistent threats, organizations are turning to threat hunting strategies that involve continuously searching for threats using various resources. Strategies may include items such as data security analytics and automated threat hunting software. The software can take advantage of artificial intelligence to review millions of data logs to identify potential threats. Human analysis is then used to make sense of the data and apply an understanding of how attackers operate.

To establish a threat hunting program, organizations first review their own assets in order to establish goals. These assets can include proprietary research, customer lists, and other sensitive information that criminals want to access and exploit. Next, organizations look at past threats and review external threat intelligence to develop a plan and determine the most effective techniques to employ. Finally, companies must ensure their teams have the required skills to hunt and identify threats on an ongoing basis.

Source: Rubens, Paul. *How to Run a Threat Hunting Program,* eSecurity Planet, May 17, 2019. https://www.esecurityplanet.com/threats/threat-hunting.html.

THE DO-OVER: CISO BEST PRACTICES

In an informal collection of observations based on a series of CISO discussions, Ray Pompon (Principal Threat Researcher Evangelist at F5 Labs) noted several basic lessons-learned themes noted on his Help Net Security article *CISOs: What would you do over?*

Best practices include:

- Plan: with clearly defined goals and a simple plan aligned with business goals, CISOs can save time and a lot of work, plus keep up with the pace of business.
- Foster Projects and Get Help When Needed: Employ good project management to mitigate risk, maintain compliance, and continue to grow programs. When you need help or resources, get what you need.
- Know Your Audience to Instill Change: Understand organizational influence across the organization, particularly when working with senior executives. This includes staying business focused and not veering into tech speak.
- Remember Physical Security and Disaster Recovery: Look beyond IT security.

Source: Pompon, Ray. *CISOs: What would you do over?,* Help Net Security, May 16, 2019. https://www.helpnetsecurity.com/2019/05/16/ciso-do-over/.

UNDERSTANDING USER ACCESS TO APPLICATIONS AND SYSTEMS

Single Sign-On (SSO)

SSO enables a user to log in once to be authenticated and then access multiple applications. It provides additional security by authenticating each user by not just using the input username and password, but also other information, including IP address, location, time of day, device, Apple FaceID, or last login.

Enterprise-level password managers

These types of password managers use a global console to manage users across the organization using security standards and policies, while providing a seamless user experience with access to a variety of the enterprises applications. The difference between SSO and enterprise password management is the central-management function with administrative capabilities to enforce security standards.

Multi-Factor Authentication (MFA)

To allow access to sensitive information, MFA is used to verify a user's identity via input of personal information (e.g., PIN, responses to personal questions, token information), smartphone verification, or through biometrics like a fingerprint or retina scan.

Source: Robb, Drew. *What Is Single Sign-On, and How Can It Make Your Enterprise More Secure?,* eSecurity Planet, March 15, 2019. https://www.esecurityplanet.com/applications/single-sign-on.html.

8913482-M-Online (09/19)