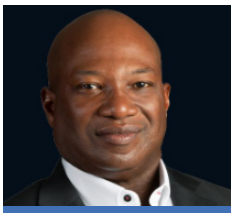
precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 17 January 2023

Security Concerns of Hybrid Work Environments and BYODs



Dr. Ronald Walcott
Managing Director

Today we will look at the security concerns of Hybrid work environments and BYODs on a company's network.

As a user-centric movement, the trend of BYOD (Bring your own device) and WFH (Work from home) is impossible to stop completely. Many businesses now operate in a hybrid environment where they allow employees to have a traditional office environment and also work from home, ever since the covid-19 pandemic. With this hybrid environment now taking over and becoming more prominent in most companies, it also brings along significant security risks and concerns for companies. Today we will look at some of these risks that companies face when they operate with BYOD policies and hybrid environments and explore effective solutions that can help mitigate those risks.

SIGNIFICANT BYOD RISKS ORGANIZATION FACE

BYOD presents a complex security problem. For example, employee-owned endpoints/devices typically contain personal information in addition to company information. It can be difficult to control and mandate users to configure, use certain applications, etc when employees use their personal devices for their work-related activities. Below are some BYOD risks listed:

- **Insufficient employee training:** A major difference between BYOD and other mobile device policies is the amount of control it gives employees. However, this can be costly to the organization especially if the employee is trusted with the data security of sensitive information. Inexperienced or untrained employees could put the organization's secure data at risk. It has been reported that social engineering attacks, which are attacks where the threat actor manipulates people into supplying sensitive information, has increased by a staggering 270% over the past couple years.
- **Data Compromise:** When employees use their own devices for work, they may need to save some sensitive information, documents etc on their devices, and this opens up the attack surface for the organization. Any access to the enterprise network from BYODs is a risk. Threat actors can gain access to the device if there are not proper restrictions, protective software, firewall, etc on these devices, especially if it is

In this Issue:

lost or stolen. Employee devices can be compromised by attackers through phishing attacks and even enterprise data by stealing data stored locally as mentioned before, stealing and using employee credentials which gives them access to the network and by corrupting or destroying the data on the endpoint.

- **Malware:** It is very common for mobile devices to be infected by malware and the user be unaware of the infection. Users often download many applications on their endpoint devices that they rarely use and don't consider the permissions and privileges they have granted to the applications. Attacks can utilize these permissions and privileges as a gateway to covertly observe/monitor, steal information or even disable systems.

HOW TO MITIGATE BYOD RISKS?

Even though the risks of BYOD are significant, it doesn't seem realistic to assume that BYOD policies would ever go away. As technology develops and people become more comfortable with it, employees will bring them to work and connect to the corporate network. This is why there must be strategies employed by organizations to combat the risks involved with employees using their own devices. Some of these strategies are listed below:

- **Device Management System:** Device management solutions keep track of each device and attach it to personally identifiable employee data. These systems can also remotely access, provide authentication services and even handle remote data wiping in the case of a device being lost, stolen or compromised.
- **Continuous Employee Training/ Retraining**: Organizations should have a BYOD policy in place and also invest in continuously educating employees on the best practices which should be stated in the BYOD policy. Employees need to know and understand what they can and cannot do on their personal devices while on the company network and premises. Employees must also be made aware of the consequences of violating the policy in place.
- **Zero Trust Approach:** Zero trust model is one which recognizes that a security approach can occur at any time to any employee regardless of the network or device they are using. Zero trust protects corporate resources by only allowing access to authorized resources. Zero trusts ethos is "Trust nothing, verify everything" and it helps to mitigate a lot of risk by only allowing authorized access to resources.

Upcoming Events

ISMG ENGAGE-FINANCE
February 16, 2023
New York

ISMG ENGAGE
March 7, 2023
Toronto

CYBERSECURITY SUMMIT: NORTH AMERICA-EAST
March 21, 2023
New York

Frequently Asked Questions:

DO BYOD RESTRICTIONS HAMPER AN EMPLOYEE'S ABILITY TO OPERATE AT THEIR FULLEST?

An organization would and should have all the resources provided that they need for an employee to effectively carry out their role. However, at times, employees feel more comfortable and operate efficiently when they use their own devices. If an employee is using their own devices, organizations usually make policies with this in mind to protect themselves and their information while not reducing productivity.

HOW OFTEN DOES A CYBER-ATTACK HAPPEN BECAUSE AN ATTACKER USED AN EMPLOYEE'S PERSONAL DEVICE AS A GATEWAY TO THE ORGANIZATION'S NETWORK?

Attackers try any and every way to get access to an organization's network and resources. If there are more people using their personal devices to work, then it will increase the possibility of attackers getting in through these devices.

ARE THERE BENEFITS TO BYOD POLICY?

As with everything, there is a positive and negative side to them. There are some positives to the BYOD policy such as increased employee productivity, reduced operating costs, higher employee satisfaction, and easier communication. However, there are always gonna be security risks involved, so businesses would have to decide if they are willing to take on the risk or not.

Headline News

T-Mobile Says Hackers Stole Data of 37 Million Customers

UNAUTHORIZED PARTY OBTAINED ACCESS TO COMPANY API FOR APPROXIMATELY 6 WEEKS

The third-largest wireless carrier in the United States told federal regulators Thursday that it found a threat actor syphoning the identifying information of 37 million customers.

T-Mobile, the name assumed by the company that emerged after the 2020 merger of telecoms Sprint and T-Mobile US, minimized the breach's impact in a filing with the Securities and Exchange Commission. No payment card, government identifiers or passwords are part of the breach, said the company. The Bellevue, Washington telecom has more than 110 million customers.

It fingered an application programming interface that exposed data including names, emails, phone numbers and birthdates as the source of the breach. Hackers did not obtain a full data set of every one of the 37 million individuals affected, it added. Prepaid and subscription customers are affected; hackers also obtained data including the number of lines on the account and service plan features.

Hackers had access to the API for approximately six weeks until company personnel spotted and shut down outside access to the interface on Jan. 5. A separate press release says the time from incident detection to resolution was less than 24 hours.

Although not as damaging as leaked financial accounts, leaked data such as phone numbers and email addresses can still pose threats to consumers, especially if bad actors know that the information is recent and therefore likely to be valid. The risk of phishing and identity theft attempts typically rises in the wake of data breaches even if cyberthieves lack information such as passwords.

The carrier only months ago entered into a $350 million settlement stemming from a 2021 breach of personal data affecting 77 million customers. As part of the settlement, the company pledged to spend at least an additional $150 million to improve its cybersecurity.

Thursday's regulatory filing says the company began in 2021 a "substantial multi-year investment" into cybersecurity and asserts the company has "made substantial progress to date."

Still, the incident may end up costing the company a significant amount in expenses, T-Mobile said.

Source: www.databreachtoday.com