K2's Security Risks And Solutions Roundtable

Learning Objectives

Identify leading cybersecurity risks that businesses face today

List examples of critical solutions you should consider implementing

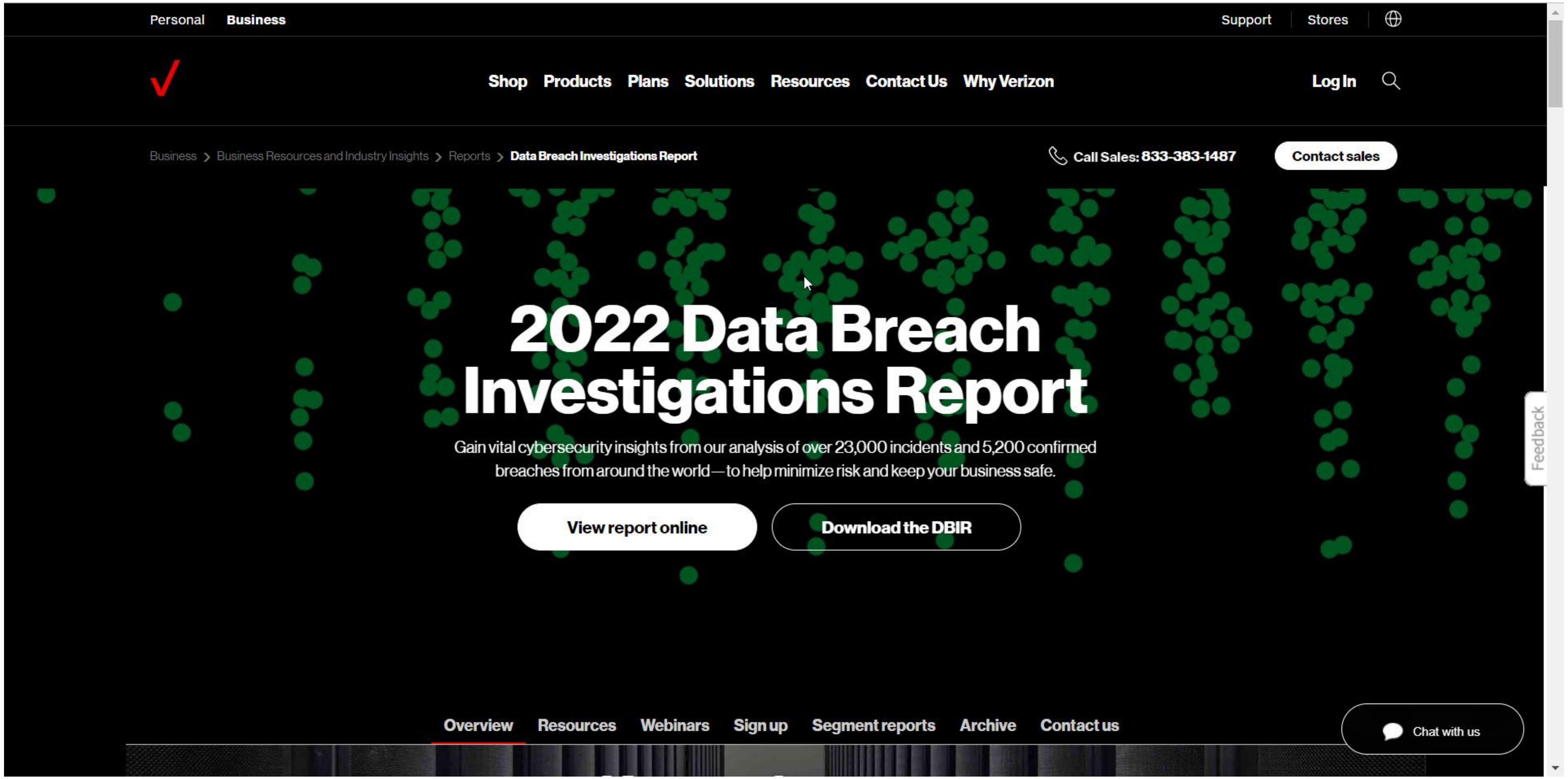
Differentiate between risk and solution profiles, depending on the size of a business

WHAT ARE TODAY'S MAJOR CYBERSECURITY RISKS?

A Sampling Of Risks…

1. Ransomware
2. Phishing attacks, including “spearphishing” incidents
3. Credential compromises
4. Poorly configured end-user devices
5. Misconfigured organizational security devices
6. Lack of appropriate security policies and plans in place
7. Inadequate team member training on policy objectives
8. Remote work environments
9. Poor backup strategies
10. Continuing to use legacy hardware and software

First, A Great Resource!



Personal Business

Support Stores

Shop Products Plans Solutions Resources Contact Us Why Verizon

Log In

Business > Business Resources and Industry Insights > Reports > Data Breach Investigations Report

Call Sales: 833-383-1487

Contact sales

2022 Data Breach Investigations Report

Gain vital cybersecurity insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.

View report online

Download the DBIR

Overview Resources Webinars Sign up Segment reports Archive Contact us

Chat with us

Feedback

PRACTICAL SOLUTIONS YOU SHOULD CONSIDER TO REDUCE RISK

Ransomware

- **NEVER CLICK** on links or attachments in email messages unless you know who sent the message and you were expecting the link or attachment
  - Consider having your email platform "strip" links and attachments
- Test compliance using tools such as **KnowBe4**, **PhishMe**, or the tool available in some Microsoft 365 subscriptions
- Enable **Controlled Folder Access** (**CFA**) on Windows-based devices to contain a ransomware attack if it occurs

Ransomware

Action Items

1.
2.
3.
4.
5.

Phishing/Spearphishing

- Carefully consider how much information you should share through social media platforms
    - Some of that info could be used to reset passwords or make a stranger seem like a long-lost friend
- Use email filtering solutions to block phishing emails from reaching targeted users’ inboxes
- Be wary of emails containing numerous typographical errors, misspelled words, urgent deadlines, or ask you to share or verify personal information

Phishing/Spearphishing

Action Items

1.
2.
3.
4.
5.

Credential Compromises

- Update password policy to match recommendations from NIST
- Mandate password management tools
- Enable multi-factor authentication (MFA) wherever possible
- Ensure team members do not share log-ins
- Block access from unknown devices and unknown IP addresses

Credential Compromises

Action Items

1.
2.
3.
4.
5.

End-User Device Configuration

- Anti-malware tools
  - Signature-based, heuristic-based, or both?
- Operating system and application updates
- End users not logging in with Admin rights
- Enabling Controlled Folder Access on a Windows device
- Mobile Device Management (MDM) tools
- Personal VPN solution
- Drive encryption, perhaps with BitLocker
- Other?

End-User Device Configuration

Action Items

1.

2.

3.

4.

5.

Organizational Devices

- Ensure only authorized users have physical access
- Restrict the number of users with administrative rights and privileges to the bare minimum
- Disable unnecessary services
- Periodically conduct penetration tests
- Verify routers, firewalls, and other devices are appropriately configured, and firmware remains updated
- Consider implementing a **Zero Trust Security Model** (ZTSM)

Organizational Devices

Action Items

1.

2.

3.

4.

5.

Zero Trust Security Models

- ZTSMs are a relatively new concept in the field of information security, but one that is receiving growing attention
- Four fundamental premises of ZTSMs
  1. Identity verification for users and devices
  2. Network segmentation
  3. Endpoint security
  4. Grant least privileges to users
- The **Edward Snowden case** provides a vivid example of how failing to implement ZTSM can lead to a massive breach

Zero Trust Security Models

Action Items

1.
2.
3.
4.
5.

Creating And Training To Policies

- Get necessary security policies in place and continually update them to match contemporary risks
  - An excellent place to start could be **The SANS Institute's Security Policy Project** (www.sans.org/information-security-policy)
- Train team members to the requirements of these policies, and make sure they understand why specific actions are necessary
- **Recognize this is an ongoing, never-ending process**

Creating And Training To Policies

Action Items

1.
2.
3.
4.
5.

Secure Remote Work Environments

- This is an often-overlooked area of concern that has escalated obviously since March 2020
- Team members working remotely should be held to the same security standards as those working in a corporate office
- VPNs, anti-malware tools, MFA, physical control of devices, Wi-Fi security, operating system and application updates, etc. are every bit as necessary when working remotely as when working in the office
- Create checklists and ensure compliance with the lists

Secure Remote Work Environments

Action Items

1.
2.
3.
4.
5.

Address Backup Strategies

- Though not popular to say, we’re probably talking about **WHEN** the breach happens, not **IF** it happens
- Therefore, focus on what recovery would look like
- Do you have an updated **Business Continuity Plan** and a **Disaster Recovery Plan**?
  - Yes, these are two different plans!
- What are some examples of things that should be in each?

Address Backup Strategies

Action Items

1.
2.
3.
4.
5.

Update Legacy Devices And Apps

- Your technology plan should address appropriate replacement cycles for hardware and software
- "Legacy" devices and apps can create security risks
  - For example, maybe the manufacturer no longer makes firmware updates available
- As a rule of thumb, any hardware used for over ten years may be beyond its useful life
- Likewise, any software that no longer is supported should likely be replaced

Update Legacy Devices And Apps

Action Items

1.
2.
3.
4.
5.

Summary

- Cybersecurity risks abound and, unfortunately, you probably cannot eliminate this risk
- However, considering the issues discussed in this session and the solutions suggested, you can mitigate cybersecurity risk to a prudently acceptable level
- Remember that risks continue to evolve and, therefore, your action plan must evolve also, or it will become outdated
- Addressing cybersecurity risk is not a project; instead, it is a process

OTHER ITEMS TO CONSIDER

Other Items To Consider

Action Items

1.
2.
3.
4.
5.

THANKS FOR JOINING US TODAY!