usecure

Prevent Data Breaches and Phishing Attacks

usecure's Guide to Dark Web Security

Table of contents

EXECUTIVE SUMMARY

The Dark Web presents significant, often underestimated risks to businesses. Sensitive company data—such as credentials, intellectual property, and customer information—can end up on Dark Web marketplaces, where they are sold or traded for malicious purposes.

Notably, 81% of organizations have experienced malware, phishing, or password attacks, emphasizing the human element as a critical vulnerability. Furthermore, ransomware activity is projected to cost victims $265 billion annually by 2030.

This whitepaper explores these threats and provides actionable insights into how businesses can mitigate risks through proactive security measures, including employee training, Dark Web monitoring, and cybersecurity protocols offered by usecure.

Introduction to the Dark Web

The Dark Web is a hidden part of the internet that requires specific software like Tor to access. It operates in contrast to the surface web (publicly accessible) and the deep web (non-indexed but legitimate). Although the Dark Web hosts illegal marketplaces and forums, it also offers anonymity for cybercriminals trading in stolen data, malicious software, and other illicit goods.

- **2.7 million daily visitors** accessed the Dark Web in April 2023, highlighting its scale and potential risks to businesses.
- Nearly **57% of Dark Web content** is illegal, including cybercrime forums, drugs, and illegal marketplaces.

Common Dark Web Threats to Businesses

Businesses face multiple risks from the Dark Web, where login credentials, personally identifiable information (PII), and intellectual property are bought and sold. Common threats include:

- **Data breaches:** For instance, the Shields Healthcare Group breach a**ffected 2.3 million individuals.**
- **Social engineering attacks:** Over **40% of successful** attacks were Business Email Compromise (BEC) or CEO Fraud imposter scams, underscoring the human vulnerability factor.

Global ransomware is predicted to cost

$265 Billion

by 2031.

$1.5 Trillion

the amount earned by cybercriminals for cybercrime activities yearly

Risks Posed by the Dark Web

Stolen data—gathered through phishing attacks, malware, or compromised systems—often finds its way to the Dark Web. This data is used to infiltrate businesses or enable social engineering attacks.

- 68% of breaches in 2023 involved a human element, emphasizing how internal vulnerabilities often lead to data exposure on the Dark Web.
- The median time for a user to fall for phishing emails is less than 60 seconds, indicating the rapidity with which attacks can succeed.

Financial, Operational, and Reputational Impact

Businesses face severe consequences from Dark Web exposure, including:

- **Average cost of a data breach:** $4.88 million globally, with U.S. companies experiencing the highest average cost at $9.44 million.
- **Nearly half of organizations report breach costs exceeding $1 million.**
- **Ransomware is projected to cause $265 billion in damages annually by 2030.** This underscores the significant operational disruption these attacks can cause.

How Data Ends Up on the Dark Web

Data often finds its way to the Dark Web through common vulnerabilities:

- **Weak Password Policies:** Inadequate password strength and reuse can leave systems vulnerable.
- **Phishing Attacks:** Deceptive tactics trick users into revealing sensitive information.
- **Insider Threats:** Malicious insiders or accidental human error can compromise data.

Employee errors or poor security hygiene remain frequent causes of breaches. 88% of cybersecurity breaches are attributed to human error.

The Role of Employee Negligence

Negligence, such as poor password management or falling victim to phishing scams, significantly contributes to data being stolen and sold on the Dark Web. Organizations must address this through proactive employee training and robust cybersecurity policies.

Mitigating the Threat of the Dark Web

usecure's uBreach and uBreach Pro monitoring tools help companies detect when their data has been exposed on the Dark Web. Early detection allows for swift action, mitigating potential damage and preventing breaches from escalating.

- **uBreach**: Offers proactive Dark Web monitoring for early warnings when credentials or sensitive data are compromised.
- **uBreach Pro**: Provides enhanced Dark Web monitoring services, with real-time threat intelligence and advanced monitoring of illegal Dark Web activity targeting specific industries or companies.

Password Hygiene and Credential Protection

To combat credential theft, companies should implement robust password management and protection strategies, including:

- Two-factor authentication (2FA)
- Password management software
- Employee training on password best practices

usecure provides password hygiene training through its uLearn platform, ensuring employees understand how to maintain secure credentials and avoid common pitfalls that lead to data breaches.

68%
of all breaches in 2023 involved a non-malicious human element

Employee Awareness and Training

Human error is one of the primary entry points for Dark Web breaches. usecure's uLearn platform delivers comprehensive security awareness training to help employees recognize phishing attacks, avoid malicious links, and follow cybersecurity best practices. Continuous education ensures employees are up-to-date on evolving threats.

- **uPhish**: usecure's simulated phishing tool allows businesses to conduct phishing simulations, helping employees recognize and report suspicious emails. Regular simulations reduce the likelihood of employees falling for real phishing scams.

Policy Management

- usecure's **uPolicy** solution helps organizations maintain strong cybersecurity practices by managing and enforcing security policies across teams. Ensuring that policies are updated and adhered to is crucial for preventing breaches and maintaining a secure business environment.

50%

of employees are unaware of their company's cybersecurity policies and procedures

$5.09 Million

the highest cost of a data breach in U.S.A in 2023

Monitoring and Protecting Against Dark Web Threats

Best Practices for Data Protection

To safeguard against Dark Web threats, businesses should implement the following best practices:

- **Data encryption:** Protect sensitive data from unauthorized access.
- **Regular security audits:** Identify and address potential vulnerabilities.
- **Dark Web monitoring tools:** Use tools like uBreach Pro to detect and respond to threats early.

Continuous Improvement and Proactive Measures

To stay ahead of evolving cyber threats, businesses should:

- **Utilize Dark Web monitoring tools:** Continuously monitor the Dark Web with uBreach Pro.
- **Educate employees:** Provide ongoing training through uLearn and test awareness with uPhish.
- **Manage security policies:** Implement effective security policies with uPolicy to maintain compliance and prevent security gaps.

Leveraging usecure's Solutions

uLearn for Security Awareness Training

usecure's uLearn platform provides comprehensive training on identifying phishing emails, preventing credential theft, and protecting business data. It has proven effective in reducing employee vulnerability to cyberattacks.

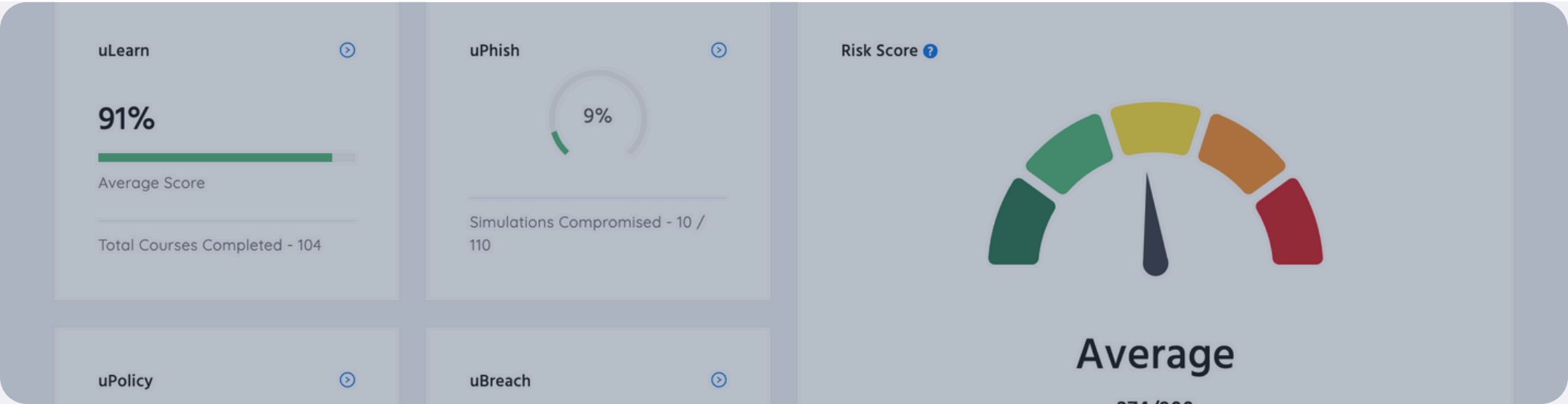
uPhish for Phishing Simulations

With uPhish, businesses can conduct phishing simulations to help employees recognize suspicious emails. These simulations enhance overall awareness and decrease the likelihood of falling victim to real-world attacks.

uBreach for Dark Web Monitoring

uBreach monitors the dark web for exposed employee email accounts and identities disclosed through third-party breaches. For enhanced monitoring, the premium uBreach Pro adds advanced features, including:

- Domain-wide breach monitoring with real-time alerts
- Exposed data snippets to detect password reuse risks
- Breach resolution tracking
- Prospecting tools for MSPs



6-Step Framework for Mitigating and Proactively Protecting Against Dark Web Threats

This framework provides a structured approach for businesses to mitigate risks and protect themselves from Dark Web threats effectively

1. Risk Assessment and Awareness

- onduct a cybersecurity risk assessment to identify weak points such as poor password hygiene, untrained employees, or outdated systems.
- Audit sensitive data (e.g., PII, credentials, intellectual property) to determine what could be exposed in case of a breach.
- Educate leadership and employees about Dark Web threats to foster awareness of risks and impacts.
- Use tools like Dark Web exposure audits to assess current vulnerabilities.

2. Strengthen Authentication and Data Protection

- Implement multi-factor Implement multi-factor authentication (MFA) across all critical systems and platforms.
- Enforce strong password policies (e.g., unique and complex passwords).
- Use encryption to protect sensitive data at rest and in transit.
- Deploy endpoint security tools to safeguard devices from malware and unauthorized access.

3. Proactive Monitoring

- Use Dark Web monitoring tools (e.g., uBreach and uBreach Pro) to identify when employee credentials or company data appear on Dark Web forums or marketplaces.
- Monitor for real-time alerts about breaches, password reuse risks, or malicious activity targeting your organization.
- Regularly review reports to understand trends and potential vulnerabilities within your industry or network.

4. Employee Training and Awareness

- Deliver cybersecurity awareness training through platforms like uLearn to educate employees on recognizing phishing attempts and other common threats.
- Conduct simulated phishing exercises using tools like uPhish to test and improve employees' ability to identify malicious emails.
- Regularly update training content to reflect emerging threats and evolving cybercriminal tactics.
- Create a culture of reporting where employees feel encouraged to flag suspicious activity.

5. Policy and Incident Response Management

- Develop and enforce comprehensive cybersecurity policies, including guidelines for password management, data access, and incident reporting.
- Use tools like uPolicy to automate and manage the updating and enforcement of policies.
- Create and test an incident response plan for data breaches, focusing on containment, notification, and recovery.
- Schedule regular security audits and drills to ensure preparedness and policy adherence.

6. Continuous Improvement and Collaboration

- Regularly review and update cybersecurity strategies to align with emerging threats and technological advancements.
- Partner with Managed Security Service Providers (MSSPs) or cybersecurity consultants to gain access to advanced threat intelligence and expertise.
- Participate in industry forums and threat-sharing networks (e.g., ISACs) to stay informed about sector-specific risks.
- Invest in cybersecurity R&D to adopt cutting-edge tools, AI-based threat detection systems, or automation technologies.
- Conduct regular post-incident reviews to analyze breaches or near-miss events, incorporating lessons learned into updated protocols.

GBH's Global Cybersecurity Strategy with usecure

About GHB Group

GBH, a multinational organization, needed to maintain cybersecurity compliance across diverse regions while managing a large, global workforce. The complexity of adhering to various regional regulations posed significant challenges.

The Solution

GBH leveraged usecure's platform to implement:

- **Localized Training Content:** Tailored cybersecurity training modules that addressed specific regional compliance requirements.
- **Automated Policy Management:** Streamlined processes for updating and enforcing security policies across different jurisdictions.
- **Comprehensive Compliance Tracking:** Tools that provided real-time insights into compliance status and potential vulnerabilities.

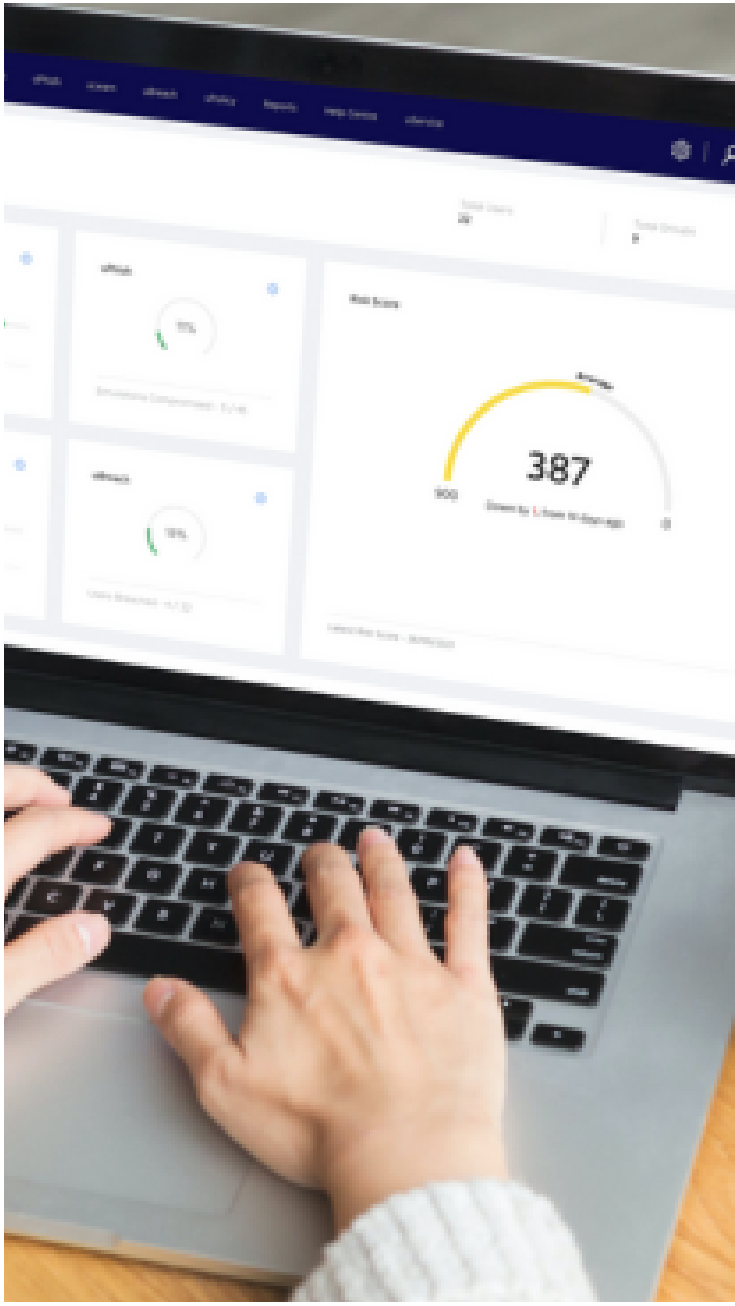
Results

GBH successfully achieved:

- Consistent cybersecurity awareness across all regions, enhancing their global security posture.
- Efficient management of compliance requirements, reducing the risk of regulatory breaches.
- Improved employee engagement with security protocols through relevant and localized content.

By utilizing usecure's solutions, GBH was able to navigate the complexities of global cybersecurity management effectively, ensuring robust protection against Dark Web threats.

Read full case study here



CONCLUSION

The Dark Web poses a serious threat to businesses through stolen credentials and data breaches, which lead to financial and reputational damage. Organizations must adopt proactive measures, such as security awareness training, strong password policies, and continuous Dark Web monitoring, to safeguard themselves from these risks. Solutions like usecure's platforms provide an essential defense, helping businesses protect their data and minimize Dark Web-related incidents.

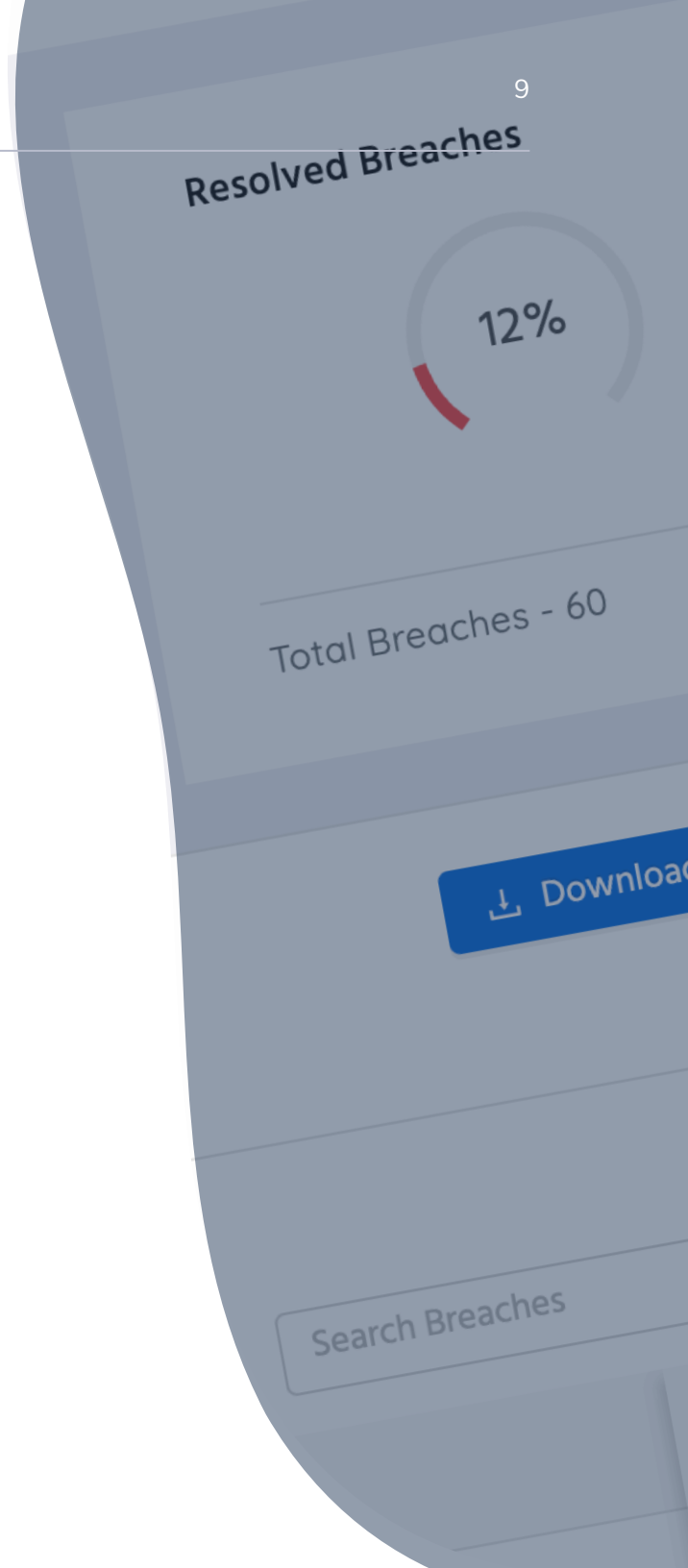
Start securing your business today by exploring usecure's Dark Web monitoring and phishing simulation solutions. Empower your employees with the training they need to defend against evolving cyber threats.

Get Started with usecure

Empower your organization like Mentor Group did. Explore how usecure's award-winning Human Risk Management solution can enhance your cybersecurity strategy.

Want to see our human management risk platform in action? **Book a demo today.**

This case study demonstrates how strategic implementation of usecure's solutions can lead to significant improvements in cybersecurity awareness and compliance.



Appendix

1. Verizon. (2024). Data Breach Investigations Report (DBIR).
2. SOCRadar. (2023). End-of-Year Report.
3. UK Government. (2024). Cyber Security Breaches Survey.
4. Allianz. (2024). Risk Barometer.
5. IBM. (2023). Cost of a Data Breach Report.
6. Fortinet. (2023). Security Awareness and Training Report.
7. Prey Project. (2023). Dark Web Statistics and Trends.
8. Positive Technologies. (2023). Financial Industry Security Interim Report.
9. Varonis. (2023). Cybersecurity Statistics.
10. Kroll. (2024). Data Breach Outlook.
11. Risk Management Monitor. (2024). New Studies Highlight Sources, Patterns of Data Breach and How to Do Better.

usecure