How to Prevent Breaches Caused by Negligent Employees

Devolutions

THE ENEMY ISN'T JUST HACKERS WHO POPULATE THE DARK WEB

Everyone knows that the cyber threat landscape is constantly getting worse. But what may come as a surprise is that the enemy isn't just hackers who populate the dark web. It's also negligent employees who populate the workforce.

According to the 2019 Insider Data Breach survey commissioned by Egress and conducted by Opinion Matters, 79% of IT leaders believe that in the last 12 months their own employees have accidentally put company data at risk. Even more eye-opening is that 55% of employees who deliberately — but not maliciously — shared data against the rules did so because their company failed to provide them with the necessary tools. Furthermore, 29% of employees didn't even feel like they had broken the rules because they mistakenly believed they had ownership of the data they had worked on — and not their company.

Examples of Data Breaches Caused by Employee Negligence

There is no shortage of horror stories linking negligent employees with costly data breaches. Here are some examples:

- The notorious Equifax breach that exposed the personal information of 145 million people was traced back to a single employee who failed to heed security warnings and didn't implement necessary software fixes.
- An employee working for the City of Calgary in Alberta, Canada, accidentally sent an email to a colleague in another municipality that contained highly sensitive and confidential information for more than 3,700 employees. The city has since been sued for $92.9 million.
- An employee at a nursing home in Northern Ireland took home an encrypted work laptop, which was later stolen — exposing protected data for dozens of patients and employees. The nursing home was fined and publicly criticized by investigators for "having totally inadequate provisions for IT security and procedure and poor data protection training".

Preventing Negligent Employee-Caused Data Breaches

The bad news is that there is no way to 100% prevent negligent employees from causing data breaches — just as there is no way to 100% prevent all cyber threats. The attack surface is just too vast, there are too many vectors, and there will always be vulnerabilities.

The good news, however, is that companies can — and given the cost and consequences of a breach, they really must — be proactive and create a defense-in-depth plan that significantly reduces both the likelihood and severity of data breaches caused by careless employees, as well as those that are deliberately launched by rogue operators and external hackers.

While each company needs to develop its own plan based on their specific threat exposure risk factors and compliance requirements, it should generally include the following mix of non-technical and technical controls:

- Provide company-wide cybersecurity education, ideally through an online training platform that can evaluate employees and target training accordingly. For example, many employees have a big knowledge gap when it comes to following good password policies.
- Identify and analyze all privileged accounts, and ensure that access complies with the Principle of Least Privilege principle (POLP).
- Implement Role-Based Access Control (RBAC), which gives employees permission to the accounts and assets they need — but nothing more. According to research by Thycotic, 40% of organizations use the same security for privileged accounts as standard accounts.
- Audit and analyze off-boarding practices, and ensure that departing employees are fully removed from systems upon departure.
- Require account owners to certify that they still require privileged at regular intervals.
- Implement Segregation of Duties (SoD), which prevents employees from having to wear "too many hats" at work.
- Generate detailed logs and reports to constantly monitor all privileged account usage and enforce strict controls for sharing credentials. According to research by Thycotic, 50% of organizations do not audit privileged accounts.
- Enforce multi-factor authentication (MFA) to enhance account security on all desktops and endpoints. Research by Forrester has found that on average, employees use 2.3 devices for work purposes.
- Use account brokering, which lets employees log into privileged accounts without needing to view passwords. A survey by Centrify found that 74% of data breaches start with privileged credential abuse.
- Require employees to store passwords in secure vaults instead of through insecure methods. A survey by Digital Guardian found that 39% of people write down their passwords on a piece of paper, and 10% keep passwords in a file on their computer.
- Adopt the "four-eyes principle", which requires that any activity by an employee that involves material risk must be reviewed and confirmed by a second employee who is independent and competent.
- Conduct a periodic criminal background and credit check to prevent high-risk employees from accessing sensitive data and mission-critical systems.

How We Can Help

Our solutions Remote Desktop Manager, Devolutions Password Hub and Devolutions Password Server help organizations secure and control the IT chaos in their environments — which also means preventing negligent employees from accidentally wreaking havoc. Key built-in features include strong Role-Based Access Control, support for 2FA, enhanced PAM functionality, and more. Plus, our solutions are affordable for SMBs and available in a variety of licensing options.

To learn more, please contact our team at sales@devolutions.net, and they'll be happy to provide you with further information based on your organization's specific needs and goals.