Stickley on Security

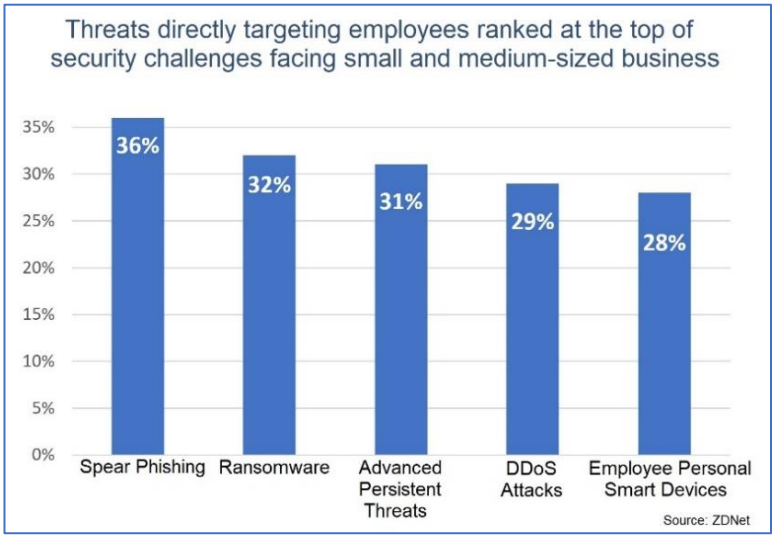
Powered Cybersecurity Training

Automated Cybersecurity Education and Phishing Simulation

Powered Cybersecurity Training™ (PCT) is designed to help solve the challenges small and medium-sized businesses face in attempting to deploy and manage cybersecurity education and phishing simulation. PCT is completely automated, including all reporting and notices. It's simple to set up your users to provide your entire organization with more comprehensive cybersecurity training than 82 percent of all other American companies.

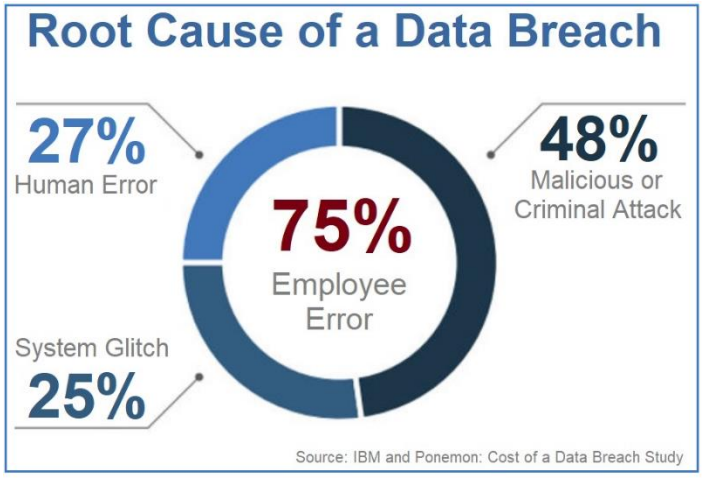
Overcoming Security Education Problems ▶

Who has the time? Other solutions are very labor-intensive, eating up valuable resources that are better used elsewhere. PCT provides a ***best-of-breed system that requires absolute minimum setup and maintenance***.



Cybercrime is continually evolving: Technology is constantly changing, which means that cybercriminals are constantly adjusting their tactics to keep pace. The experts at SoS keep their collective finger on the pulse of cybercrime, ensuring that everything we issue, from monthly phishing emails to quarterly education courses, is based on the latest cybersecurity measures and countermeasures. This ensures that ***your cybersecurity training is never outdated*** and that your employees stay equipped to deal with whatever cybercrime efforts they face.

Infrastructure is not a complete solution: It's clear that firewalls, encryption, and other infrastructure measures, while important, do not offer complete protection against cybercrime. Tens of thousands of dollars' worth of cybersecurity infrastructure can be circumvented by just one employee clicking the wrong email. Various studies indicate ***somewhere between 70 and 90 percent of all data breaches start with a phishing email***. The most effective way for businesses to combat cybercrime is to include comprehensive cybersecurity training with their technology solutions.



Most cybersecurity education is boring and outdated: PCT is designed to be interesting and engaging. But most importantly, it's designed to provide current information. Whether a new employee starts today or a year from now, you're assured that they ***receive the most up-to-date cybersecurity training on the market***.

Underestimation of very real security threats: SMBs often assume that they're "flying under the radar" when it comes to cybercrime. Nothing could be further from the truth. ***Cybercriminals often target smaller organizations*** knowing that the smaller the firm, the more likely they have weak cybersecurity. PCT ensures that every employee, from senior executives down to the clerical staff, is aware of the serious cyberthreats with which your organization is constantly faced.

Powered Security Training Components ▶

Complete and comprehensive education: SoS releases a ***completely new cybersecurity course every quarter*** based on the then-current cybersecurity landscape. Each course includes a video, written content, gamified interaction, and a quiz. Our multimedia approach ensures that all learning styles are addressed. Automated notices remind users to complete the course and automated reporting keeps management updated. For companies with an existing Learning Management System (LMS), we can provide courses in an industry standard SCORM-compliant file.

Topics covered: PCT covers a ***broad range of topics***, including general cybersecurity, malware (all devices), social engineering (remote and on-site), fraud, scams, and how to handle confidential data and personal identifiable information (PII).

Randomized monthly phishing emails: Our best-practices approach to cybersecurity demands that phishing simulations be run monthly. The look and feel of each email we send is unique so that they aren't easily recognizable as simulations by employees. Also, a variety of emails are sent randomly over the course of each month to allow employees to experience the test on their own and make it more difficult to be warned of the email by others. Most importantly, each email is based on current phishing tactics, ensuring that your employees are presented with real-world simulations. ***PCT customers invariably experience a dramatic reduction in failure rates, typically below five percent, after just three months of use*** and maintain that rate or lower even as employees come and go.

Training assigned to failed phishing tests: When an employee fails a phishing test, it's an indication that they require additional training. The PCT system ***automatically assigns a relevant training module to any employee who clicks a phishing email***. We send a weekly notice to the employee until they complete the module and full reporting/monitoring is provided for the system administrator.

Automated and Detailed Reports: The ***PCT system emails an overview report each month to keep administrators aware of phishing and education statistics***. Administrators can also generate and download comprehensive reports any time from our full-featured customer portal. Our reporting engine has a clickable scoreboard that provides a quick look at your organization's overall statistics. Drilling into the results is simple, with several filters to refine results. Filtered results and full reports can be export to PDF (Acrobat) and CSV (Excel) formats.

Employee Training Programs Fall Short

Only 50% Agree or strongly agree that current employee education programs actually reduce noncompliant behaviors

43% Provide only one basic course for all employees which often don't cover a number of large risks that lead to data breaches

Organizations Need to Foster a Culture of Security

Only 33% Provide incentives to employees for being proactive in protecting sensitive information or reporting potential issues

32% Have no consequences if an employee is found to be negligent or responsible for causing a data breach

Source: Ponemon

www.StickleyOnSecurity.com
800.640.6743