wombat security technologies
Change Behavior. Reduce Risk.

Global Manufacturing Company Reduces Malware Infections by 46%

Wombat's Security Education Platform is changing behaviors, reducing infections, and lowering remediation costs

THE CHALLENGE

A large international equipment manufacturer based in Pennsylvania needed to come up to speed on security awareness. Though things were clicking on all cylinders from a business perspective, the company's new information security officer was concerned that security training for its employees was virtually non-existent — and he was worried that knowledge gap would become an issue sooner rather than later.

"Any company that is not taking awareness seriously is hedging its bets," he said. "In my opinion, the single most important thing an organization can do is create a security awareness program."

The information security officer made awareness a top initiative, and he took up the charge of convincing the company's Board of Directors that his goals were important and would be beneficial in the short term and over time. "I recognize that sometimes you need to build awareness about your awareness program," he said. "Even though we are a 100-year-old company, we only started discussing cyber-security concerns about a year ago. And to their credit, our Board members recognized that companies were struggling to get their arms around the cyber-security realm."

In explaining the need for a more engaged and aware employee base, the information security officer shared a persistent and increasing problem the company's technicians were facing: phishing emails.

"We have a very strict email authentication program in place for all incoming messages. Unfortunately, though it's great for filtering out spam, it's not been terribly effective at preventing phishing emails from getting through," the officer said. "Those emails were a prime source for infections, but we also had a number of employees exposed to malware in online browsing sessions. They simply weren't recognizing some of the dangers in the sites they were visiting and the files they were choosing to download."

> **"Any company that is not taking awareness seriously is hedging its bets."**

Without an understanding of how to spot and avoid phishing emails and online traps, employees were falling for scam messages, clicking suspect Internet ads, and visiting malicious websites. Naturally, these activities had a negative impact on the company's internal systems. At times, the organization was dealing with more than 70 malware infections a day worldwide. The information security officer estimates that cleaning each infected PC costs the company's IT departments more than $35, which put remediation costs at nearly $700,000 per year.

After sharing the phishing data and benchmark vulnerability studies with the board of directors, the information security officer was given the green light to implement a training program for the manufacturer's global employee base — and reduce the risks associated with lack of awareness.

THE SOLUTION

The information security officer began his search for a suitable program, knowing that he was looking for a solution that would engage employees and allow him to actively measure the effectiveness of the company's efforts. "It's very important for our Board, obviously, that we show results," he said.

In addition, the manufacturer needed training that could be efficiently delivered in multiple languages. The organization consistently translates all its corporate communications into multiple languages in order to offer a seamless experience to the employees in their home locations. It was critical for the company to be able to maintain that approach with any training materials.

After exploring a few different options, the security officer found what he wanted in the Wombat Security Education Platform. Wombat's approach resonated with him because it meshed with his desire to use education and awareness to drive behavior change while measuring results.

"We looked at some others solutions, and there were a few things that made Wombat stand out from the rest. The platform is easy to use, and the graphical user interface and management system make it really easy to pull stats. Plus, we can easily customize and deploy the mock phishing messages. We saw some great comfort in those features," he said. "We also appreciated Wombat's more 'formal' and business-like approach to the vendor relationship, which we didn't see with some of the other companies we researched. It's what we look for in companies we engage with."

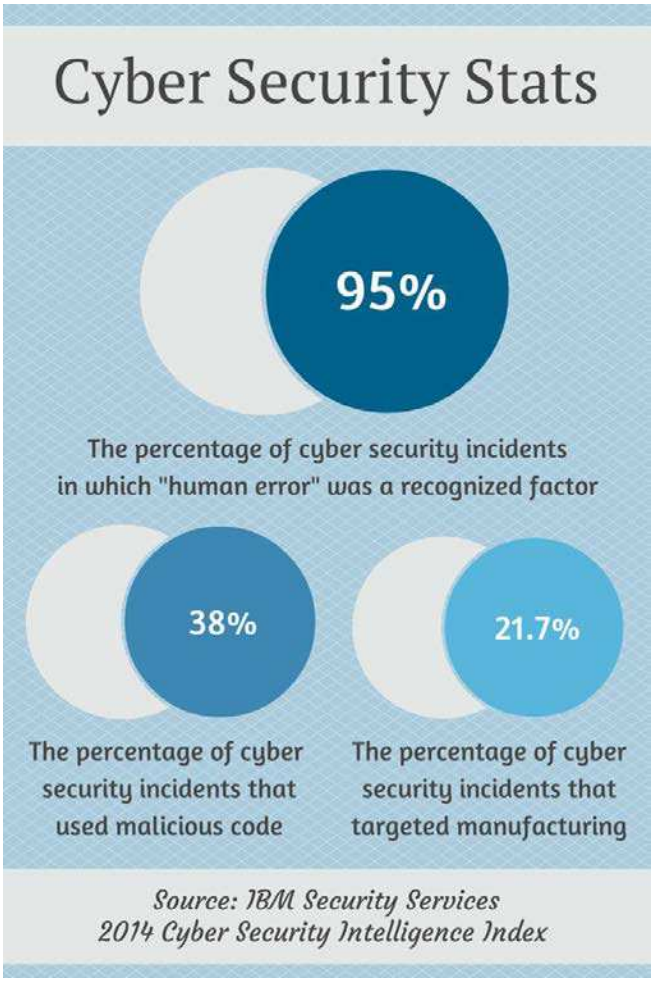
With Wombat, the organization had the flexibility to tailor its approach to security training, using both interactive educational modules and threat assessment tools. The manufacturer agreed that this multi-faceted methodology presented the best opportunity to change employee behaviors and build a lasting defense against cyber threats.

Implementation

The Wombat Security Education Platform was an ideal fit because it allowed the organization to lead with training rather than focusing solely on mock attacks. The company already knew it had a problem with phishing emails and malware downloads, and the information security officer had identified data points tied to frequency of infections. From the outset, one of the biggest initiatives in his mind was awareness. He wanted to put that in motion right away to help the company's employees make the right decisions when they came in contact with security threats.

In its initial phase, the company rolled out training to its 5,000+ global employees with a focus on three key areas: safer web browsing, email security, and URL training. The training was voluntary, but employees in all location were encouraged — and reminded — to complete the modules.

Following this rollout, the security information officer began to utilize Wombat's PhishGuru® simulated attack tool. Though the company knew they had an issue with phishing messages, they had been unable to pinpoint the types of emails that were most likely to garner a response — or which employees in which locations were most susceptible to these kinds of attacks.



Wombat's support team worked with the manufacturer to ensure the mock phishing messages would not be intercepted by its email filter. The customizable messages were sent to different departments over a two-month period, with each department receiving the mock phishing emails over a span of several days. This feature was very appealing to the organization.

"I believe random scheduling is a key to more accurate results," said the information security officer. "We have open cubicle environment in many of our locations, and I think varying the delivery helps reduce the number of instances in which employees will warn their colleagues not to open a certain message." If everyone were to get the same message at exactly the same time, he said, it would be a red flag for employees and result in a skewed picture of the organization's vulnerability to attack.

Because the Wombat Security Education Platform is an all-in-one delivery and analysis tool, it can measure results during and after every phase of training and assessment, enabling security officers to evaluate where weaknesses are and respond accordingly. Training cycles, mock attacks, and knowledge assessments can be repeated at targeted intervals, increasing the chances of long-term risk reduction.

THE RESULTS

"We have had some very positive feedback from the Board and our end users regarding the training and the simulated phishing messages," said the information security officer. "People really love the interactive nature of the modules. As an R&D company, we like to think that we have a pretty educated workforce, and the employees seem to appreciate the deeper dive. I don't think we would have been able to achieve this level of awareness using the materials from some of the other companies we researched."

46% Reduction in Malware Infections Globally

Prior to the start of training, the company was experiencing 72 malware infections daily throughout the organization. Just four months into the program, the company saw that total drop to 39 infections, a 46% reduction. The organization's European locations saw the most significant change, with a 69% reduction in malware infections following the first cycle of voluntary training. Overall, the reduction translates into a potential for more than $300,000 in annual savings on remediation costs.

> **"We've developed a healthy sense of paranoia. I think that's the best result that can come out of the awareness training we're doing."**

Fewer Helpdesk Calls

Before training, the organization's helpdesk received an average of 32 calls a month related to spyware, virus, and malware concerns. After four months, that monthly average decreased to 20, a reduction of 40%.

Buy-in From the Board

Because the reporting features of the Wombat Security Education Platform are so robust, the security information officer has been able to share important insights with the Board of Directors. "I've been able to show them the training response rates and give them a very clear picture of the vulnerabilities we have with phishing," he said. The Board had visibility into the types of mock emails that were being sent to the employees; which departments and employees were falling for the attacks and what they were clicking; and the types of information employees were sharing when prompted to do so.

"I think the reason we're getting such great support from our Board is because we're able to show results on the things we're doing," said the information security officer. "But the potential for cost reductions isn't really the driver here. To me, it's rooted in awareness. I feel this kind of work is essential to a secure work environment, and the Board concurs with that."

LOOKING FORWARD

Because the education and assessments have been so well-received by end users and the Board of Directors, the goal is to transition from voluntary training to mandatory training. “We definitely plan on using the tool more and getting more modules out to our user base,” the information security officer said. “And at a recent meeting with the Board, they seemed intent on making the training mandatory.”

The company intends to roll out four to six additional modules in its next year of training, and the information security officer would like to incorporate Wombat’s CyberStrength® Knowledge Assessments in addition to ongoing simulated attacks. He will also be working with managers throughout the organization to do targeted attacks within certain departments. The goal is to use the data and analysis to help those managers better address and counter security threats that are specific to the activities and responsibilities of their teams.

The company has seen a quick return on its investment in the Wombat platform. The reduction in malware infections and helpdesk calls has freed up company resources, and the potential for significant savings on remediation costs is a great proof point for the program. But the security information officer points to the increase in awareness and change in employee behavior as the most significant results from the Wombat training and assessments.

“The results we’re achieving and the positive feedback we’re receiving because of our engagement with Wombat is going a long way with our Board of Directors. We have really raised security awareness here, and that’s something we didn’t have a lot of,” he said.

“Conversations are happening, people are talking to each other about emails they’re receiving, they’re thinking about phishing and the potential consequences. We’ve developed a healthy sense of paranoia throughout the organization. I think that’s the best result that can come out of the awareness training we’re doing.”