EXECUTIVE BRIEF

Creating a culture of security

CYBERSECURITY

Executive summary

Creating a culture of security is a challenge most organizations face, but which many struggle to properly address. As a global enterprise software company that provides products for every aspect of business, Infor's first step in tackling this problem was to first assess its corporate culture to identify key problem areas and to understand its employees' mindset. To implement its findings, Infor® implemented a phishing simulation tool, developed in-house security awareness training, refreshed its communication strategy, and made it easier for employees to find and understand security-related information. These initiatives have so far resulted in increased reporting of security incidents and suspicious emails, higher employee engagement, a decrease in click rates on phishing simulations, and an uptake in employees taking optional security awareness courses.

A comprehensive security awareness strategy is critical to any organization's success. Employees have access to internal information, resources, and systems that must be protected from cyber threats. To achieve a significant impact on employees' attitudes and behavior, security must be embedded into the corporate culture.

Introduction

It's no secret that a comprehensive security awareness strategy is critical to any organization's success. Employees have access to internal information, resources, and systems that must be protected from cyber threats.

Approximately 70% of security incidents caused by employees are a result of human error, negligence, or insufficient training.[1] Phishing, malware infections, and other social engineering attacks use manipulative techniques to trick people into performing an action against their best interests. Data spills, poor password management, and system misconfigurations are other human factor-related incidents.

While there is no way to eradicate human error, it is possible to significantly reduce the amount of incidents caused by negligence and insufficient training with the right security awareness strategy. Some organizations perceive security awareness as a mostly-useless formality meant to fulfill compliance standards and keep stakeholders happy.
This mindset is unlikely to have any kind of real of effect on employee behavior, and can lead to wasted resources or a failed program.[2]

In this paper, we explain how Infor is tackling the human factors in cyber security and how we are continuously monitoring and improving our security awareness strategy. We discuss the importance of assessing the corporate culture as it already exists, and how to go about gathering such information. Next, we explain how we used this information to begin embedding security awareness into the company culture so that employees understand the importance of cyber security and how to protect themselves and their data from common attacks.

Along with customer-first initiatives that strive to continuously improve the customer experience, Infor also places a high priority on protecting customer data. The techniques and experiences outlined in this white paper can also be transferred to help you develop a better security awareness strategy for your organization.

Key components of a successful security culture

Policies. To take policies seriously, employees must be able to understand them. Policies must be clear, easy to locate, regularly updated and vetted, and accompanied by documentation that outlines proper compliance. New hires must be trained on security policies during on-boarding and receive refreshers and updates throughout employment. More importantly, management must consistently communicate and enforce policies, as commitment to policy can have a ripple effect.

Management support. To gain managerial support to ensure funding and enforcement of a security culture, it's important to present a compelling business case with security-related metrics, a plan to align changes with business objectives, and key performance indicators. Costs should be justified against the financial impact of non-compliance or a potential breach.

Personal, environmental, and social factors. The more an employee identifies with an organization, the more inclined they are to follow its policies. Promoting a culture of personal well-being, flexibility, and understanding can help to significantly reduce the likelihood of a breach resulting from stress or poor health. This should naturally improve compliance. Other cultural factors include the quality of working equipment and office space, investment in training, promotion of work-life balance, and offering of benefits.

Education, training, and awareness. Often, security programs fail due to inadequate research on corporate culture and a lack of insight into the root causes of employee behavior. Education efforts are ongoing, and require consistent outreach through multiple channels to cater to different learning styles. Programs should be measured and re-evaluated against your organization's needs. Most importantly, security awareness should focus on positive messages where employees understand what is expected of them, how to adhere to company standards, and why it's important.

Assessing the corporate culture

To achieve a significant impact on employees' attitudes and behavior, security must be embedded into the corporate culture. Corporate culture is shaped by the shared assumptions, values, and social norms of the people within it, and often affects how team members perceive react to corporate change and practices.[3]

Before implementing any changes, it is crucial that you build an in-depth understanding of your corporate culture as it currently exists. Assessing your corporate culture can help you identify potential opportunities and challenges in the process of pursuing a security initiative. It helps you understand how employees think, what motivates them, and how they perceive the company. Infor used the following tools to assess its own corporate culture:

Security culture surveys

Security culture surveys are a great way to develop an initial idea of your employees' behavior and perceptions, as they can highlight the strengths and weaknesses of the current corporate culture. Since most surveys are not compulsory, employees may require further incentive to participate, whether it involves a reward for the first 100 people to complete it, or escalation to the line manager for those that do not complete it. This is a good opportunity to test whether reward or punishment schemes are more effective for your organization.

Focus groups

Security culture surveys are limited to quantitative information, so hosting focus groups enables you to gain richer insights into the rationale behind your employees' answers. From here, you will gain valuable and actionable insights into what your employees need in terms of security awareness and motivation. It is easy for focus groups to go off topic while in session, so it is recommended you follow a structured methodology such as **Interactive Management** to keep topics focused and relevant whilst also keeping the discussion open enough to explore a wide variety of phenomena.

Analysis

Most survey tools can analyze quantitative data, but qualitative data gathered from focus groups will require an analysis method such as thematic analysis or **content analysis**. Without this, it will be difficult to organize the data in a way that makes sense.

Findings

When we at Infor conducted an assessment on our own corporate culture, we gained a wealth of ideas on how to improve communication and increase engagement. Our primary areas for improvement included:

Underdeveloped reward structures

Our results showed Infor as having many aspects of a healthy corporate culture already in place. Many surveyed employees felt a sense of belonging at Infor, and when employees feel a strong organizational commitment, they are more willing to exert effort into following best practices and policies while protecting Infor's assets. On the other hand, employees expressed that Infor lacked a recognition and reward scheme for individuals who go above and beyond when it comes to cyber security.

Need for tailored education and training

In addition to computer-based security awareness training, employees said they wanted more training that was specific Infor's way of working, as opposed to the generic and off-the-shelf courses in our Learning Management System (LMS). They expressed a desire to have training that was specific to their departments' unique requirements. Additionally, they wanted training to be delivered in-house from a member of the security team.

Lack of documentation and communication

Responses from our security culture survey showed many employees were unsure about where to find security policies and documentation, as well as who to contact with security-related queries. Employees are required to read the information security policy every year upon completing security awareness training, but if they needed to refer back to it they often forgot where to find it.

These findings demonstrate the importance of conducting internal research instead of rushing into security awareness initiatives, which is where many organizations can fail. For example, an off-the-shelf security awareness program will deliver an abundance of training resources, but employees are unlikely to pay them much attention if what they really want is company-specific, in-house training. Additionally, off-the-shelf products cannot tackle communication issues within an organization. By taking time to analyze cultural aspects and bring employees into the discussion, we gained incredibly valuable insights and action items.

Changes and improvements

By learning more about our employees' needs and behaviors, we were able to implement a variety of solutions that help cultivate a culture of security.

Phishing simulations

To educate employees about real-life security awareness situations, we began running simulated phishing attacks on their work email accounts. By providing them with a simple Outlook add-on that allows them to report suspicious emails, we've helped team members get an idea of what to look for in potential phishing attacks, as well as how to report them in the workplace. When employees use the add-on to report non-simulated emails, a dedicated team investigates the email and reports the outcome back to the employee who reported it. When a genuine phishing email has been identified, it is remediated and tracked for further activity.

In-house security awareness webinars

The security team now hosts security awareness webinars for each department to provide a customized training experience for employees. Careful consideration of cognitive psychology has been applied to the design of the webinars, allowing us to present key messages in a way that helps prevent information from being forgotten and encourages acceptance of the information presented. Each session addresses the most common issues that specific departments face, reiterates our security policies, and is kept to a maximum of 30 minutes to prevent cognitive overload. We primarily focus on showing employees exactly how to work securely in our environment using the tools available to them. Employees can ask questions at the end of each session, which helps familiarize them with the security team so they know where to go if they have any concerns or queries.

Improved on-boarding for new hires

When new hires join Infor, they are required to take our annual security awareness training as well as two short training videos on phishing simulations and how to analyze suspicious emails. They are required to read and agree to our information security policy and shown where to find other policies, how to report security incidents, and are provided with links to internal security related resources.

Intranet site for security

Prior to this study, the security team had an internal security site, but it mainly hosted technical information that was only relevant to development or customer-facing teams. We have since launched a separate intranet site that is open to all employees where we share information such as news on the security team's projects, information on the security tools we use and why we use them, links to our security policies, training resources, and much more. This site is now the one-stop place for all security related information, and its bookmark is loaded on to employee's laptops by default in the build process.

Streamlined submission process

To make our security efforts more accessible, we have made it easier and more intuitive for employees to submit security incidents or concerns. All the information they need to know is hosted on the security intranet site with step-by-step instructions and reiterated in our internal security awareness webinars. We've also included a way for employees to submit concerns anonymously for instances where they might be worried about retaliation.

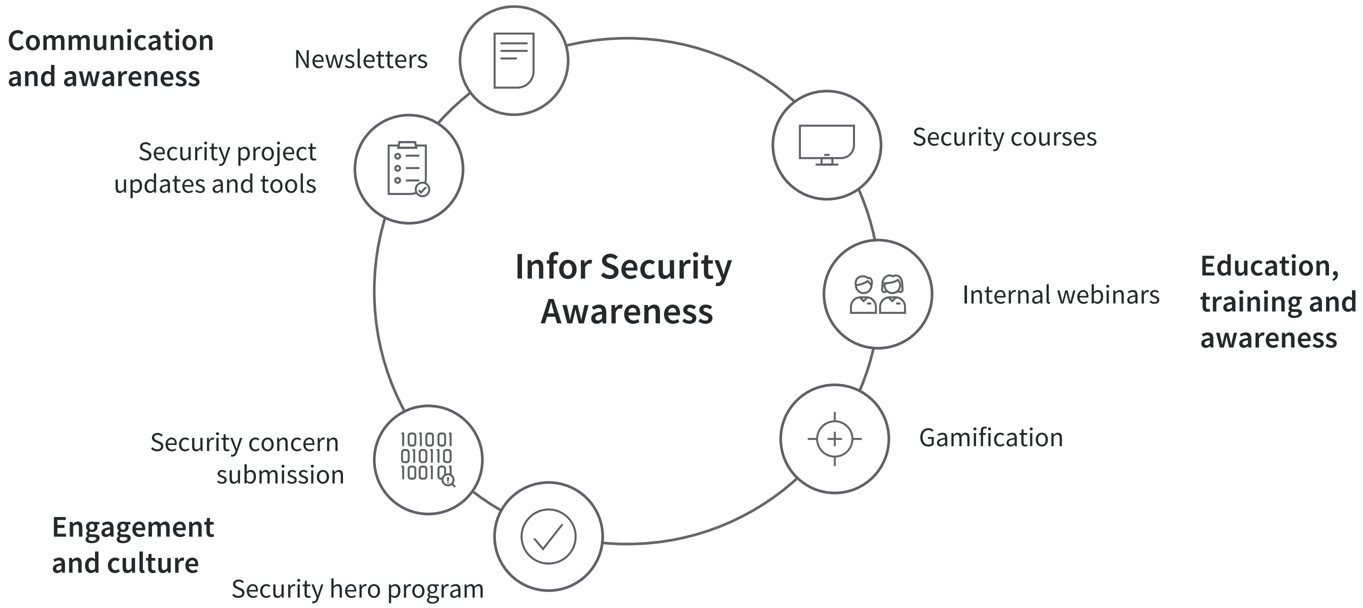
Security Hero program

To reward employees who help improve Infor security, we developed the "Security Hero" program to recognize employees with exceptional participation in our security efforts. Employees can nominate each other based on one of five security-related values through an online form. When a nomination is submitted, it automatically notifies the employee's manager of their achievement and then they are assigned a badge in the employee system. Each quarter, we select a few winners from the list of nominees and present them with an award and a shout-out in the security team's newsletter.

Newsletter

Security is often seen as being a culture of "no" that hinders productivity. We use newsletters and other communications to promote security in a positive way to help adjust this negative perception to one that is helpful and aims to provide solutions instead of criticizing mistakes. Infor's security newsletters keep employees up-to-date on the security team's project initiatives, new security tools, the latest security best practices, common scams that are circulating, and recognize teams or individuals that have contributed to the improvement of Infor's security.

Figure 1. Infor's security awareness strategy



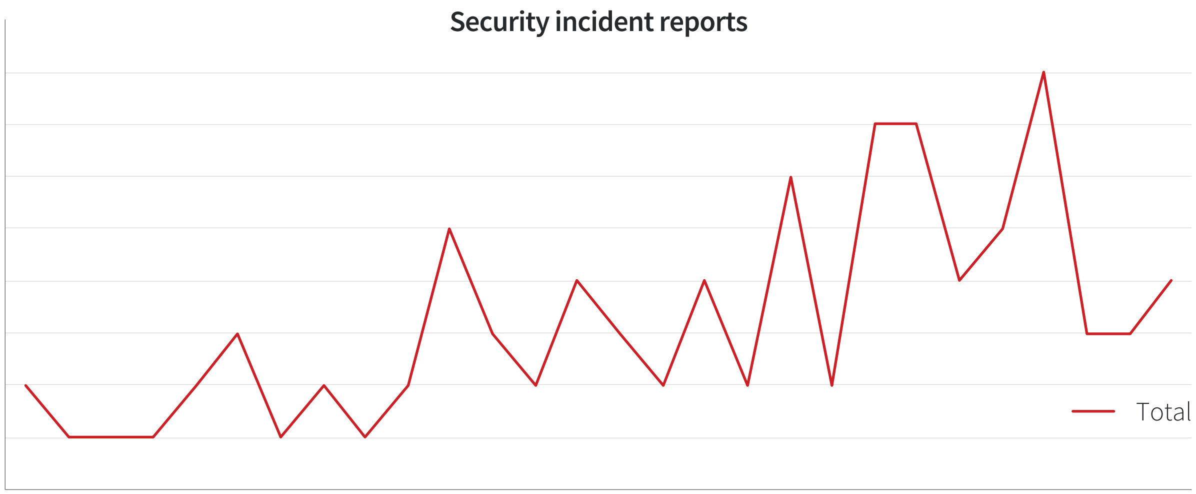
Gamification

To ensure adoption of security best practices, it’s important to use training methods that work for different learning styles. Some people prefer to learn via person-led webinars, others prefer computer-based courses or reading, and some people enjoy learning through games and competitions. Gamification is a fun and interactive learning method that has been shown to improve engagement. We introduced a range of security-based gaming courses and held a company-wide friendly competition that utilized leader boards for a competitive edge. Our most recent gamified experience was in celebration of National Cyber Security Awareness Month (NCSAM). Employees were given a variety of security-related activities to participate in, which earned them points for their department.

Impact

Since refreshing our security awareness strategy, we have seen a significant improvement across multiple areas. The number of reported non-phishing related security incidents has risen by 750% since 2017. We attribute this to an improvement in communication and visibility to the security team through our newsletters, security awareness sessions, and resources hosted on intranet site.

Figure 2. Rise in reported security incidents between 2017 and 2020.



We have also experienced a huge rise in the reporting of suspicious emails. Since implementing a one-step phishing report button, the number of emails being reported has grown by over 1000%.

Previously, employees had to submit an IT ticket for suspicious emails, but the convenience of the one-step method is encouraging people to report more emails.

Figure 3. Increase in reported emails. Manually submitted IT tickets vs Outlook add-in.

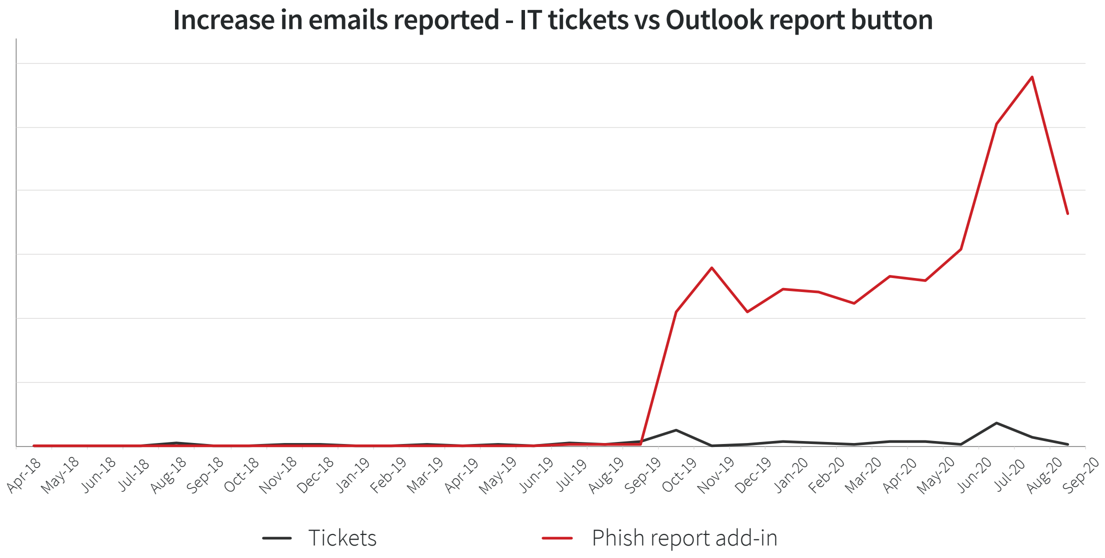
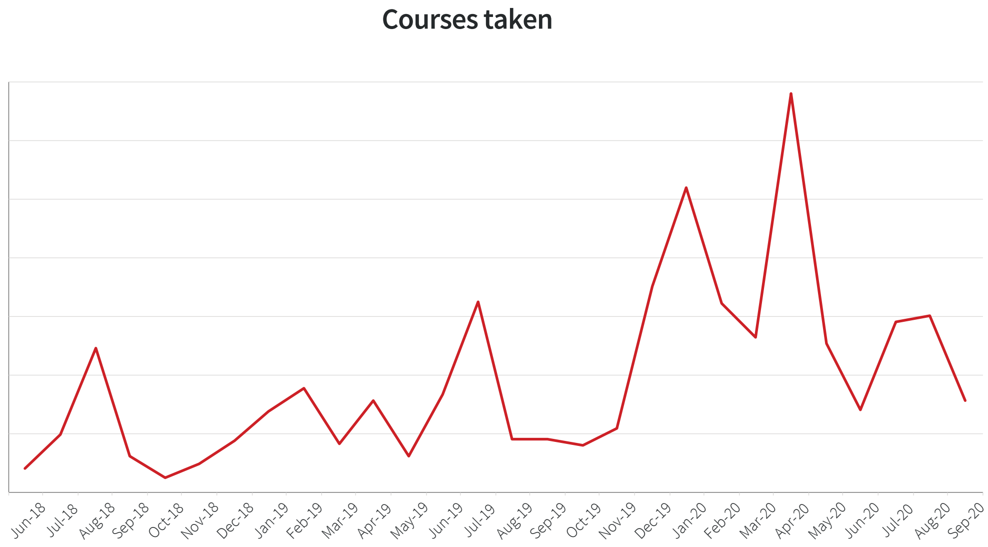


Figure 4. Rise in optional security awareness course participation since 2018.



With our mixture of department-specific and company-wide phishing simulations, this year we saw a 5% - 33% decrease in click rates across multiple high-risk departments and we are seeing higher report rates compared to click rates. For example, in our most recent global simulation, 24% more people reported the simulated phishing email than those that clicked.

In April 2019 we introduced a system for recognizing employees for investing their time in optional courses where their manager is also notified. This has had a positive effect on the amount of participants, and has also increased engagement.

Conclusion

When it comes to cybersecurity, under-informed employees can present a massive vulnerability point. But an education, training, and awareness program in itself is not enough to transform employee attitudes and behavior—instead, security must be embedded into your corporate culture for maximum effectiveness. When you assess your organization's culture as it already exists, some of the findings may be surprising—and you might realize there are changes to make to the corporate culture as well.

Over the last few years at Infor, we have witnessed an astounding increase in engagement for security, which is not only shown in our statistics for reporting security incidents and optional courses being taken, but also some behavioural aspects that are difficult to quantify but can be felt within the culture. We have experienced an increase in employees coming to the security team for advice, as well as positive feedback following our internal security awareness sessions and recognition scheme. Despite how often they may be overlooked, a security-first culture can provide a valuable opportunity for any business dedicated to serving their customers and protecting their data.

October 2020, Jodie Ward (MSc), Risk Analyst at Infor.

References
1. Forcepoint, 2017. The Cost of an Unintentional Insider Threat.
2. D. Lacey, Managing the human factor in information security. Hoboken, N.J.: Wiley, 2009.
3. Schein, E., 2010. Organizational Culture and Leadership. 4th ed. San Francisco: John Wiley & Sons.

LEARN MORE →

Follow us:

Infor builds business software for specific industries in the cloud. With 17,000 employees and over 67,000 customers in more than 170 countries, Infor software is designed for progress. To learn more, please visit www.infor.com.

641 Avenue of the Americas, New York, NY 10011