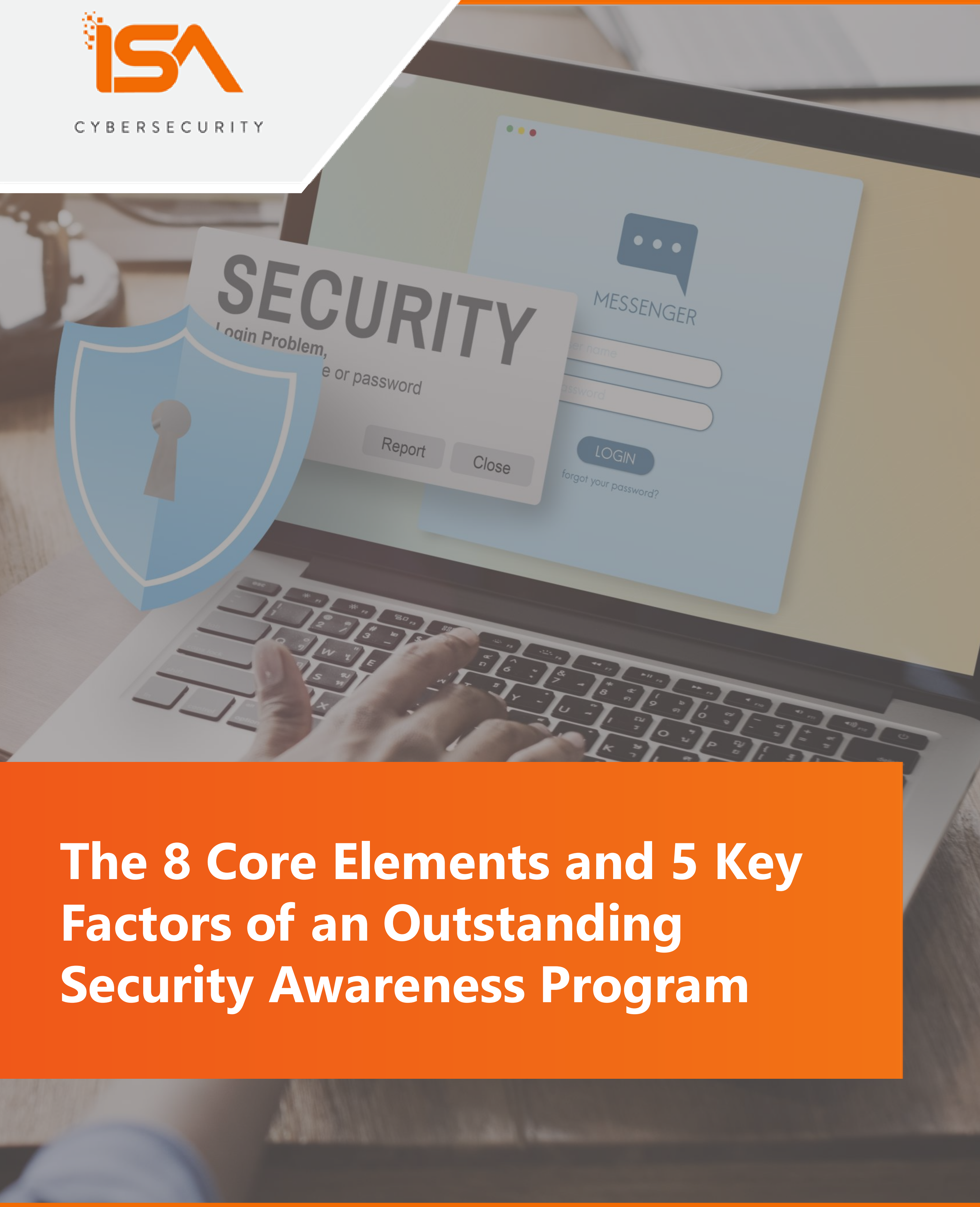
ISA

CYBERSECURITY



The 8 Core Elements and 5 Key Factors of an Outstanding Security Awareness Program

Conducting security awareness training is one of the most important ways of defending your organization against cyber risk. This ebook explores why you need an awareness program, what it should look like, and how to make it a truly outstanding part of your cybersecurity strategy.

TABLE OF CONTENTS

WHY DO I NEED A SECURITY AWARENESS TRAINING PROGRAM?

Strengthening the "Human Interface"

The Verizon 2021 Data Breach Investigations Report suggests a human element was involved in a stunning 85% of successful data breaches in 2020. Security awareness training helps increase your team's vigilance – not just by spotting phishing emails or other social engineering attacks, but by conditioning them to look critically at their day-to-day activities. A cyber aware workforce will identify and report issues like over-provisioning of permissions, unexpected error messages or suspicious system behaviour, or other "red flags" in your digital environment.

A value-add for staff

An effective security awareness program will yield benefits at work and at home for your staff. Many of the defensive techniques and strategies in your office program are immediately transferrable to the personal lives of your team members. Their home vigilance will, in turn, make them more aware and prepared for incidents in the office, in a positive feedback loop. The knowledge they get will come in handy more often than they might realize.

Compliance

Regulatory compliance is often a compelling reason for instituting a security awareness program. ISO 27000 series certifications and PCI-DSS compliance demand documented cybersecurity training programs. Audit requirements and best practice guidelines for many industries also insist on educating your staff. Moreover, most cyber insurance underwriting processes will ask you to confirm that you conduct training before they will offer coverage.

85% of successful data breaches in 2020 involved a human element

(Verizon 2021 Report)

8 CORE ELEMENTS OF AN OUTSTANDING SECURITY AWARENESS PROGRAM

1 **Recognizing phishing attacks**

Identifying phishing attacks must be one of the key skills developed in your security awareness program. The Verizon report identified phishing involvement in over a third of all successful data breaches in 2020. While spam filters, email security applications, and anti-malware software are a big part of the solution, training your staff to not click that suspicious link can be as powerful as any automated defense.

2 **Social engineering**

Phishing is just one piece of the puzzle when it comes to social engineering defenses. Your training must encourage staff to be vigilant about the risks of scams over the phone and by text. As some personnel begin to head back to the office in the waning months of the pandemic, they may have forgotten some of their defensive skills against "shoulder surfing", "tailgating" and other threat techniques in the workplace. Your training program should remind your team about these physical risks as well.

3 **Passwords and authentication**

Best practices around passwords and authentication are an important part of your training program. The key here is to ensure that your company policies support and enable the strategies covered in your training. Teach best practices about password use, and make sure your systems are aligned with those practices (e.g., in terms of complexity, password history, change frequency, etc.). Training and support for multi-factor authentication should be available for anyone handling or responsible for customer data.

4 **Handling portable devices**
Though cloud services (discussed below) and virtual storage solutions have replaced many physical storage devices in everyday use, it's still important to educate staff about the dangers of trusting unknown portable devices and ensuring that they are equally aware of the risks of "over-using" thumb drives to transfer sensitive data. Lost or unprotected USB keys can create costly data disclosures.

5 **Mobile work security**
The COVID-19 pandemic thrust "work from home" upon many organizations at an alarming speed and scope. Comprehensive security awareness training must cover the key elements of safe remote work, encompassing essentials like separation of work/personal equipment and credentials, maintaining confidentiality in shared spaces, etc. Appropriate use of public Wi-Fi falls under this category too – staff need to employ VPNs or be made to realize that any data transmission in a mall or coffee shop is an easy target for threat actors.

6 **Cloud organization**
More and more companies are relying on cloud services to cost-effectively manage their business. But the cloud has made it easy for staff to spread content around to various services and platforms (each with its own security challenges), creating risk. Staff need to understand how to secure their files wherever that data "lives" – be it on a mapped Office 365 drive, a SharePoint folder, in Dropbox or some other online storage service, in their own email boxes... or all of the above. Practical IT security policies and straightforward training on those policies will help prevent a "wild west" of unsecured copies and competing versions.

Training your staff to <u>not</u> click that suspicious link can be as powerful as any automated defense.

7 Physical security

While the cloud is increasingly the home of much of our data, the physical IT infrastructure still must be protected. Restricting access to assets, providing due care and protection for portable devices, and guaranteeing the secure destruction of obsolete equipment and media, all need to be addressed in your training program.

8 IT policy awareness

Frequently, companies will introduce corporate IT policies to new staff in their first week as part of onboarding – along with a firehose of other information. Understandably, staff may not fully absorb the elements and importance of your company's defined policies surrounding responsible computing, appropriate use of corporate resources, etc.

Your training program should remind staff that corporate data storage and equipment should only be used for company business; the same goes for internet service and email use. Best practices on social media should be addressed in your program: over-sharing information in posts (or even selfies) can create unintentional hazards for personal privacy and corporate confidentiality. Your security awareness training program, done well, will tie all these messages together.

5 KEY FACTORS TO AN OUTSTANDING SECURITY AWARENESS TRAINING PROGRAM

1 **Executive support**
The "tone from the top" is always important when getting buy-in for a security awareness program. All staff are watching the executive and management levels for how seriously they take security. Coordinated efforts from IT, HR, and internal communications will help get the word out and emphasize the importance of the program. Consider tying security awareness into your performance management process – if security training is a "goal" or otherwise acknowledged in individual evaluations, compensation, and bonuses, then staff will be more anxious to participate and do well.

2 **Awareness is a marathon – not a sprint**
It's crucial to understand that a one-off, annual PowerPoint does not constitute an effective security awareness program! The best programs are continuous, regularly delivering compelling interactive content, testing engagement and competency through online quizzes, spot tests, and ethical phishing exercises. Steady reinforcement of the messages will help deliver more than just awareness; it will eventually change the fundamental behaviour of your staff, so "cyber secure" becomes a natural way of doing things – not some kind of forced afterthought.

3 **Personalization**
Training is more compelling when it feels real. Make sure your security awareness program materials speak to the applications, business issues, nomenclature, and current events that concern your enterprise. The program becomes more engaging when staff can relate directly to the content. The spot tests and evaluations also become more challenging and impactful when they reflect real situations in your business, as staff may let their guard down.

4 Continuous improvement

Continuous refinement and improvement of your program – and your staff's awareness – is best supported by a training feedback lifecycle. A dramatic improvement in awareness and "click avoidance" on phishing tests should be seen within the first couple of training cycles; maintaining program momentum will help drive the numbers even lower. Effective programs will follow the lifecycle of:

- **Analyze:** Assess the areas of emphasis, take baselines of staff awareness and competence. Establish the KPIs you want to monitor to help quantify success.
- **Plan:** Organize and develop training materials that address the key areas of improvement or concern and are relevant and compelling for staff.
- **Train/Test:** Deliver the training materials and challenge the staff on their engagement and comprehension by testing during the sessions, followed up by spot tests.
- **Measure:** Gather and evaluate the results of your training and testing and look for trends. This moves you back into the analysis phase and the lifecycle continues.

5 Celebrate success! Follow up on failure

Aside from emphasizing the business importance and personal enrichment from cyber awareness, "gamification" of cyber awareness can be effective as well. Reward "perfect scores" on tests; acknowledge staff who recognize all the indicia of a phishing email hidden in one of your tests. Be creative. Make it fun.

But where staff have challenges or aren't absorbing the message, don't simply "re-test" them until they pass. Check in with staff who have struggled in certain areas, not to blame or shame, but to truly understand where the difficulties lie in understanding and preparing for cyber attack. This thoughtful analysis will be appreciated by staff, and help you craft better training and messaging to make your program more effective for everyone.

TAKE A FRESH LOOK AT YOUR SECURITY AWARENESS TRAINING PROGRAM

See if there are ways you can make your security awareness training program more engaging, more relevant, and ultimately more successful. Use your program to help make every member of your workforce a part of a team effort to keep your company cyber safe.

If you are looking to improve your corporate security awareness, ISA Cybersecurity can help! We provide managed training services that educate your staff while keeping the program administration and maintenance off your plate. Our solution is scalable: we have helped single office companies right up to global, multi-language customers with tens of thousands of users. Most importantly, our programs get measurable results. Our customers – ranging in size from 100 to over 34,000 users – have achieved **dramatic 80-90% reductions in "phish-failure percentage"** within a year of our security awareness training and testing process.

ABOUT ISA CYBERSECURITY

At ISA Cybersecurity, our mission is to help customers achieve their privacy and security goals, and to be proactive in the fight against security threats. ISA Cybersecurity is Canada's leading cybersecurity-focused solutions and services provider, with nearly **three decades of experience** delivering cybersecurity services and people you can trust.

GET IN TOUCH

1-877-591-6711

info@isacybersecurity.com

isacybersecurity.com

Toronto | Calgary | Ottawa