KnowBe4
Human error. Conquered.

Building a Regulation-Resilient Security Awareness Program

Building a Regulation-Resilient Security Awareness Program

Table of Contents

INTRODUCTION

International organizations of all sizes are in a never ending race with emerging cybersecurity regulations. The sheer scale and number of country-spanning cyber attacks in recent years has brought this threat into sharp focus for international governments.

The goals of these regulations are vital: reinforce cyber defenses against an endless onslaught of cybercriminals seeking data, money and reputation.

But this race can leave infosec professionals feeling left behind. The alphabet soup of directives and guidelines, such as the EU's Digital Operations Resilience (DORA) for financial institutions and the NIS2 directive, will keep most Chief Information Security Officers (CISOs) and their team on their toes.

Alongside increased technical controls and policy requirements, today's cybersecurity regulations and guidelines increasingly include security awareness training programs.

On one hand, this increased focus on security awareness and culture is a good thing, as the human element of cybersecurity is something technical controls cannot fully address. On the other hand, whether requirement or guideline, few details are typically provided on how to provide security awareness training that will change an organization's security culture for the better.

How can organizational policies keep up with ever-expanding regulations and guidelines as they get more detailed and wide-reaching? We can't say we have all the answers but we can provide infosec professionals with best practices to develop global regulation-resilient security awareness programs designed to stand the test of time.

This whitepaper provides an overview on the emergence of security awareness in international cybersecurity regulations and discusses best practices for building a security awareness training program to help prepare you and your organization for both today's and tomorrow's training and awareness requirements.

EXPLORING THE INTERNATIONAL CYBERSECURITY REGULATORY LANDSCAPE

We've put together a table with half a dozen particularly impactful regulations and guidelines and how they relate to security awareness. The table quotes chapter and verse in the given policy that mentions security awareness and notes whether each can be considered a requirement or not. Access the table here.

One element that is too complicated to present in table format is the subject of fines. Some have no objective penalties since they are guidelines (though running counter to established best practices has its own less-concrete downsides). Others, however, definitely have teeth.

The General Data Protection Regulation (GDPR) carries fines of €20 million ($21.5 million) or 4% of the business's total annual worldwide turnover, whichever is bigger. That latter number led to a record-breaking €1.2 billion ($1.3 billion) fine for Facebook parent Meta in 2023; more than all of 2022's fines combined.

The newer European directives DORA and NIS2 carry their own penalties, too. Financial institutions found in violation of DORA's requirements may face fines up to 2% of their total annual worldwide turnover. DORA also applies to specific third-party entities serving the finance industry and could levy fines up to €5 million ($5.4 million). The NIS2 Directive ups this ante with fines up to 10% of an entity's annual turnover.

Long story short: Regulators are getting serious about cybersecurity and data privacy threats, and are willing to make you put your money where their mouth is.

EVOLUTION OF THE CYBERSECURITY REGULATORY LANDSCAPE

Ultimately, these regulations are driving toward stronger, more robust protections against increasingly sophisticated cyber threats. The newer guidelines and mandates are the international regulatory community's answer to threats that transcend national borders.

The newer guidelines and mandates are the international regulatory community's answer to threats that transcend national borders.

Case in point: the NIS2 directive, which is mainly aimed at broadening the types of organizations affected in regard to the previous version of the directive (NIS1). Previously, only the energy and transportation sectors were affected. Now it covers a wide range of sectors defined as both critical infrastructure and essential services, including the digital pipelines that keep the global economy flowing. Recent high-profile cyber attacks on both critical infrastructure and supply chain interests globally have undoubtedly influenced this expansion in scope.

What NIS2 is seeking broadly, DORA is aiming at financial institutions for similar reasons. 2023 data breach cost research claims that financial institutions lose $5.9 million per data breach; 28% higher than the global average. The expected financial gain and large attack surface make this type of organization an extremely attractive target for cybercriminals. DORA's overall goal is to reduce risk associated with information and communication technology (ICT). Banks and similar entities make the world run, so European regulators want to ensure that these organizations are as risk resilient as possible.

Risk Management in Place of Threat Management

These two new and expanding directives help paint a picture of a broadening focus on risk management as a whole for regulators across the European Union and beyond.

Rather than simply reacting to threats, these evolving policies seek to shore up critical organizations of all types against risk from current cyber attacks and those to come. The inclusion of passages requiring security awareness and training programs represents acknowledgement that a robust security culture influenced by a trained workforce is an important step in a proactive cybersecurity framework.

But despite the gallons of digital ink spilled to craft these directives, they don't have much to say about the why and how of security awareness and training. That's where KnowBe4 comes in. The next section of this whitepaper will explore how to build a business case for security awareness and how to structure a program to equip your workforce with knowledge for now and the future.

MAKING THE CASE FOR PROACTIVE SECURITY AWARENESS

> *As a CISO or infosec professional tasked with complying with these regulations, security awareness and training can be your best partner.*

We at KnowBe4 consider it a good thing that cybersecurity policies and directives include specific mention of security awareness and training. More for the benefit of our customers as it only takes three minutes to hack a human. All of the technology and preventative measures your organization puts in place can be easily circumvented through a social engineering attack. As a CISO or infosec professional tasked with complying with these regulations, security awareness and training can be your best partner.

Let us explain.

One of the common issues we hear from infosec professionals in your position is the difficulty they have to make the case to their leaders on why security awareness training is needed. Well, if a directive like DORA or NIS2 includes security awareness in its very text, that's a pretty easy way to start a conversation with your leadership.

Being able to cite regulation for something as usually nebulous as security awareness right alongside the more objective, technology-based requirements can go a long way to showing your leadership that security awareness is needed and just as important.

Culture Trumps Mere Compliance

With that foot in the door, the next step is helping them see the benefit of going beyond the bare minimum requirements. One or two training courses delivered throughout the year may make some theoretical auditors happy. But will this approach serve you and the organization for years (and regulations) to come?

No it won't.

Here we're talking about the concept of improving your security culture, which is defined as the ideas, customs and social behaviors of a group that influence its security. Security culture can be considered a part of a broader company culture but requires its own specific tasks, objectives and responsibilities to achieve.

Indirectly, cybersecurity regulations that include discrete mention of security awareness can be considered an attempt to codify strong security cultures in a language C-Level executives can better understand — fines and risk management. The trick is taking this seed and encouraging it to grow.

With this starting point, emphasize with your leaders the inherent value in a culture of cybersecurity awareness. Take a proactive stance; this isn't just about threats today, but preparing for the future. A strong security awareness program builds a resilient, educated workforce that becomes not simply compliant, but truly cyber-aware.

> *Indirectly, cybersecurity regulations that include discrete mention of security awareness can be considered an attempt to codify strong security cultures in a language C-Level executives can better understand — fines and risk management.*

When making your case, speak in terms of risk management and investment. Risky employee behaviors should be managed just like any other threat to the organization. Investment to counter risk is not just expected but vital in any other aspect of the business; areas where a bare-bones approach will not cut it. The same should be true for managing risk through security awareness training. Security awareness should be pitched as an investment that protects your organization and helps ensure you're able to face the cybersecurity challenges of tomorrow.

Next up, we'll discuss some best practices for putting together a security awareness program designed to positively impact security culture.

BUILDING A COMPREHENSIVE SECURITY AWARENESS PROGRAM

We'll begin by making clear that the details of any security awareness program need to be worked out for each specific organization. No approach to security awareness is a one-size-fits-all.

That said, the lack of detail on security awareness training these regulations and guidelines often include can be a good thing. This means that a robust, engaging security awareness program designed to improve security culture (what you want anyway) will more than likely fit the bill across the board. The primary caveat to keep in mind is that industry-specific training content may be required in addition to any general program on cybersecurity (think payment card security training called out by the PCI DSS standard).

The core of a comprehensive security awareness program can be broken into three pillars:

- Organizational Needs
- Content/Communication
- Measuring Effectiveness

Let's explore each pillar one by one.

Organizational Needs

This pillar begins with doing the work to figure out what risks and requirements are relevant to your organization. The training content you will deliver, and ultimately the employee behaviors you want to influence, should align with your top organizational risks.

Remember that risk is often calculated in the formula: Risk = Likelihood × Impact, so the risk you are addressing and behavior you are modifying may not be the most common, but instead may be the most impactful.

The risk you are addressing and behavior you are modifying may not be the most common, but instead may be the most impactful.

Some choices here will be simple. To put it plainly: there's stuff you simply have to train your employees on. You'll need to think about what industry-specific training you might be required to deliver. Referencing chapter and verse that mention security awareness in the pertinent regulations will help.

Some decisions will require more research into your organization's top risks. Choosing the risks and behavior(s) to address depends on your organizational threat model and risk appetite. Referencing recent annual reports, such as the Verizon Data Breach Investigations Report (DBIR), may also provide insights into current threats which you may want to address. Internal employee knowledge surveys and interviews with IT staff will also help suss out your employees' cybersecurity knowledge and help decide where training is needed.

It's important to recognize that what you need should extend beyond what's required. Remember: you sold your leaders on improving your security culture; which goes well beyond meeting the bare minimum.

Content/Communication

Next comes the training content and cadence. A successful program shouldn't be "one and done." Treat it as an ongoing marketing/PR campaign.

Once-a-year, "check the box" training will not work toward changing user behavior. Continuously presenting the information in different ways (formal training, posters and graphics, lunch-and-learns) is what will influence their decisions and make it easier for users to make smarter choices.

The overall goal of training content is to communicate the "why" changing behavior is important for the safety of the organization.

We typically recommend at least 10-15 minutes of training content delivered per month plus one-per-month simulated phishing tests to keep the lessons top of mind. Ensure to include any required topics, even if that pushes one or two months beyond the 15-minute training mark. We also recommend engaging with security-savvy employees to become "security champions" who can help share the message person-to-person throughout your organization.

The overall goal of training content is to communicate the "why" changing behavior is important for the safety of the organization. This is called "intrinsic motivation" and is vital because we are asking employees to take additional steps to accomplish daily tasks.

Consider the example of locking a computer when you step away. While locking a computer is trivial, it also requires that you unlock it when you return. This can result in a user being required to enter their password more times throughout a workday. If people do not understand the reason for doing it, and it does not relate to them, it may cause friction.

This is why communication is vital in modifying behaviors and improving security culture. It might be beneficial to inform people of upcoming training by sending an email to employees, or even better, having an executive send it.

Effectiveness

The third pillar is gauging the effectiveness of your training efforts. Use information from your simulated phishing tests, tools that measure user risk scores and follow up knowledge assessments to see what worked and what didn't. This information should be used to focus on additional topics as needed.

> *One thing alone will not make a difference; it is the continued combination and alignment that ultimately changes behavior.*

Remember to document the results in a report that can eventually be shared as evidence with an auditor. Your leadership will also almost certainty want to know how things are going, so use this information to keep them in the loop.

Reports to executives may not need a lot of detail, but can reinforce the improvements and make future commitments from executives and management a lot easier. Be sure to include the before and after results and any discernible changes that happened as a result.

If you decide to change your focus, remember to continue reinforcing the behaviors you have been working on so they are not forgotten. One thing alone will not make a difference; it is the continued combination and alignment that ultimately changes behavior.

CLOSING THE LOOP

International cybersecurity regulations are a moving target, caused by bad actors making life harder for all of us. But we see the inclusion of security awareness in these policies as a sign of hope that the human element is being taken seriously.

The spirit of these regulations is about more than just weathering the storm; it's about being prepared. It's about investing time and thought into making sure your people aren't just up-to-date, but ready for tomorrow's challenges. You are key to championing change in your organization by ensuring it is secure and compliant with these regulations.

In building a proactive, strong security culture, the key to resilience lies not only in robust technology but in the power of an informed, vigilant workforce. Embrace continuous learning and build a security culture to protect your company against the single biggest cyber risk: the human element.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com