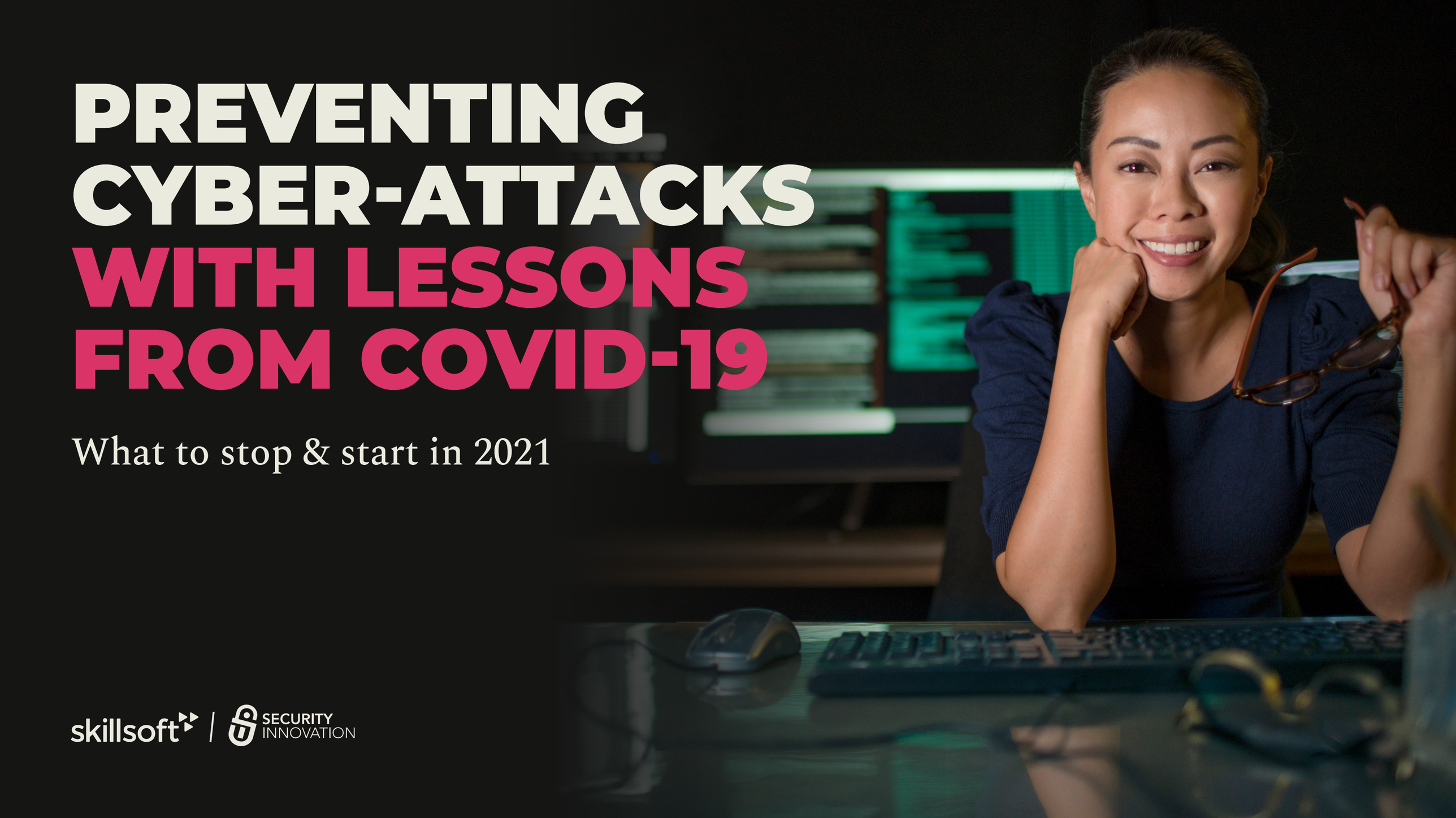
PREVENTING CYBER-ATTACKS WITH LESSONS FROM COVID-19

What to stop & start in 2021



skillsoft | SECURITY INNOVATION

INTRODUCTION

It takes more to improve cybersecurity than investing in Cloud transformation or DevOps.

Progress is achieved through continuous training, process vigilance, and tools modernization. A difficult fact to accept is that cyber-attacks are impossible to stop completely. There is too much at stake.

Despite this somber reality, you can expand protection in meaningful and measurable ways. Winning requires everyone in an organization to understand and follow basic principles for safeguarding assets. Success is a commitment from Dev and DevOps teams to fully embrace security in each job role.

At the start of the year, more than 3 million security jobs are expected to remain unfilled.*

Learning and training are effective methods for fighting off attackers. Cybersecurity isn't a fair fight. An intruder just needs to uncover one vulnerability, be patient, move laterally, and evade detection. Defenders need to protect against hundreds of known tactics, dozens of known techniques, and perhaps the most disturbing of all, the unknown.

> "Most cyber-attacks are a function of human error, lack of good training, and lack of employee attachment and commitment to staying on that training."
>
> **BRIAN DEESE, BIDEN CHAIR OF THE NATIONAL ECONOMIC COUNCIL****

*Ponemon Institute Research report, Cybersecurity Training Benchmarks, September 2020

**Source: Quote from Freakonomics podcast episode 433

OUR SECURITY MODEL RESTS ON A FOUNDATION OF BASIC PRINCIPLES SUPPORTED BY FOUR PILLARS:

As this model unfolds, you will discover some actions you need to stop that increase vulnerabilities. The model also reveals good practices to improve your odds against attacks and more efficiently allocate security resources. While mitigations can take many forms, we focus on security literacy, skills development, and reinforcement.

PREVENTION

8 LESSONS TO APPLY FROM COVID-19

Sadly, 2020 has taught each of us the necessity of thinking like an epidemiologist. We've learned more about viruses, antibodies, and vaccines than most of us cared to mention. As we progressed along our learning curve, interesting similarities arose between protections against COVID-19 infection and efforts to prevent cyber-crimes.

We experienced wave after wave of viral surges and failure after failure at performing what we knew to be effective preventative measures. Recent approvals of Messenger RNA (mRNA) vaccines have boosted our enthusiasm for reducing viral spread.

By applying some of the lessons we learned fighting COVID-19, we might be able to make progress towards better cybersecurity.

LESSONS FROM COVID-19 AND HOW TO APPLY THEM TO IMPROVE SECURITY:

BE CAREFUL WITH WHAT YOU SHARE	Protect confidential data and access to resources.
DON'T BECOME A SUPER SPREADER	Be wary of phishing attempts and e-mail attachments.
KEEP SOCIAL DISTANCE	Segment networks. Create distance in the software supply chain.
WEAR A MASK IF YOU TALK TO STRANGERS	Invaders will exploit even the smallest openings and vulnerabilities.
SANITIZE EVERYTHING	Encode and encrypt all sensitive data and confidential information.
WASH FREQUENTLY AND COMPLETELY	Keep up with security patches and updates.
VACCINATE UNTIL HERD IMMUNITY IS ACHIEVED	Everyone needs to increase security literacy and stick with learning and training. Knowledge, like antibodies, may not last long.
EXPECT VARIANTS AND EVOLUTION	Prepare to recognize new and possibly unknown threats.

Prevention is the most cost-effective approach to fighting back and the least disruptive. Threats that can't be prevented must be detected, our next pillar of the Security model.

DETECTION

8 THINGS TO STOP DOING IN 2021

MITRE is an over 60-year-old organization working in the public interest to catalog cyber-threats. The MITRE Attack Framework is a knowledge base on the web that helps organizations understand adversary groups and the tactics, techniques, and procedures (TTP) they use to invade and disrupt.

The MITRE Attack Framework has identified 291 unique tactics and more than 50 techniques. Adversaries often repeat TTP that have worked in the past, so knowing about them is a key to detection. The power of the MITRE database has been extended by open-source programs that hunt threats.

Adversary groups aren't alone when it comes to repeating behaviors. Organizations also engage in behaviors time and again that increase their vulnerability to attacks and make detection more difficult, costly, and complex.

Here are some actions organizations should stop doing to improve their overall security posture and reduce requirements for investment in detection. Detection is often unsuccessful until the damage is done.

STOP ASSUMING EVERYTHING IS SAFE

For too long, we have accepted weaknesses in the software supply chain. We must be more diligent about putting pressure on the supply chain to demonstrate proof of deep security scrutiny from third-party software.

STOP FIGHTING THE LAST WAR

The SolarWinds attack from Russia occurred because we were looking for a different tactic deployed in the past. We clamped down on hackers while the state-supported adversaries implanted malware and evaded detection.

STOP CREATING OPPORTUNITIES FOR HARMFUL SQL INJECTIONS

Web forms are a favorite entry point for intruders to insert SQL commands rather than requested information. Undetected, invaders can access underlying databases and make malicious changes to data or SQL commands.

STOP SKIPPING SECURITY PATCHES AND UPDATES

Fixes are often the consequence of vulnerabilities discovered during attacks. The difficult detection work has already been done for you.

STOP USING 3RD PARTY APIS WITHOUT SECURITY ACCEPTANCE TESTING	APIs are the most attacked code. and expose back-end systems and web browsers.
STOP CONFIGURING CLOUD DEPLOYMENTS WITHOUT ADEQUATE SECURITY POLICIES	The public cloud is safe with extensive security infrastructure. However, transitioning to cloud doesn't mean the end to security concerns. All the basic principles still apply.
STOP RAPID-FIRE DEPLOYMENT OF NEW SOFTWARE RELEASES WITHOUT PROTECTED CICD (CONTINUOUS INTEGRATION CONTINUOUS DELIVERY) DEVOPS PROCESSES	Detecting attacks is more difficult when new releases push live weekly, daily, or even hourly. Protecting Cloud systems is an example of the intersection of people, policy, and technology.
STOP ASSUMING COMPLIANCE WITH STANDARDS LIKE NIST (NATIONAL INSTITUTE OF STANDARDS) IS THE SAME AS ADOPTING SECURITY PRINCIPLES	Both are valuable but perform different objectives.

Detecting invaders is not necessarily any easier after stopping these risky practices but should reduce the volume of threats and free up resources. There are sound security practices organizations can start doing that are beneficial as well.

> **"SolarWinds was a wakeup call unlike anything we've ever seen before. This is like a Cyber Pearl Harbor. Russian actors have hands-on keyboard access to U.S. Government and private organizations all at the same time. People are now driving harmful actions. This intrusion is much more harmful."**
>
> **STEVE GROHMAN, SENIOR VP AND CTO, MACAFEE***

*Source: Bloomberg podcast 'The Tape' 29 December, 2020

ASSESSMENT

6 THINGS TO START DOING IN 2021

Assessing risk is a basic principle of security. Using sickness as a metaphor for a security intrusion, you would want an illness that is well understood, with adequate treatments and a high probability of a positive prognosis. While you can't pick your cyber-attack, you can implement good practices that reduce the risk of more damaging attacks and at the same time make more realistic assessments of risk.

ACTIONS TO START TO NOURISH A HEALTHY SECURITY ASSESSMENT:

RECOGNIZE GOOD HABITS:

Some Dev and DevOps teams see security as a primary focus. Start shifting more security responsibility left to Dev and right to DevOps as a core function and away from dedicated security job roles.

ESTABLISH A SECURITY CHAMPIONS PROGRAM:

Champions promote security literacy, quantify risks, and model good practices. Security champions are not native security professionals. Instead, they are rewarded for integrating security principles into their primary job roles. A program ensures a steady supply of new and motivated champions.

IDENTIFY ADVERSARY GROUPS ALONG WITH VULNERABILITIES:

Leverage the MITRE Attack Framework to learn about adversary group behaviors as they often repeat known attacks. Be forward-thinking.

MODERNIZE SOFTWARE DEVELOPMENT:

More software is crafted than coded. Integrate security acceptance testing into the crafting process. Leverage security routines from open-source libraries and GitHub repositories. Use machine learning (ML) as an assessment tool.

RAMP UP DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING FOR REMOTE WORK AT HOME USING THE CLOUD:

Harden your collaboration tools and usage policies. These are not temporary shifts.

MEASURE CROSS-ORGANIZATIONAL SKILLS:

You can’t improve what isn’t measured.

Assessing risks at all levels is important to understanding the types of mitigation required and the investment needed to make a real impact.

MITIGATION

5 SKILLS TO DEVELOP IN 2021

The importance of security literacy cannot be overstated and is the first line of defense against threats. In this context, mitigation is a people and skills development requirement. Skillsoft provides learning and training resources across the vast landscape of security topics. Learners will find materials at just the right level to build highly desired competencies.

SOME SUGGESTED SKILLS TO BUILD INCLUDE:

- Basic security principles and application.
- DevOps and CloudOps security features, methods and techniques.
- Attack prevention and threat detection capabilities.
- Hands-on practical experiences that challenge and test security literacy.
- Artificial intelligence (AI) and machine learning (ML) applications for security.

Skillsoft offers books, self-study materials, live online and recorded bootcamps, hands-on learning experiences with Practice Labs, Security Innovation Cyber Ranges, and more to match budding security champions' learning preferences. This list summarizes Skillsoft security content offerings:

200+ HOURS OF NEW SECURITY VIDEO CONTENT IN 2020

4 SECURITY-ORIENTED ROLE-BASED JOURNEYS

3,000 LIBRARY OF 3,000 BOOKS COVERING METHODS, PRACTICES, AND TECHNIQUES

35 CHANNELS WITH SECURITY CONTENT

24 HANDS-ON PRACTICE LABS

COMPTIA AND CISSP BOOTCAMPS (LIVE ONLINE AND ON-DEMAND)

COURSE ASSESSMENTS TO MEASURE PROGRESS

"Blended training programs yield higher security posture. The more cybersecurity training practices adopted, the higher the Security Effectiveness Score (SES). Organizations that have adopted an average of 54 percent of the training practices are in the highest SES quartile."

PONEMON INSTITUTE RESEARCH REPORT*

*Source: Ponemon Institute Research report, Cybersecurity Training Benchmarks, September 2020

CYBER RANGE:

Skillsoft content partner, Security Innovation, provides a powerful learning experience that challenges a learner's understanding of security in a fun, yet highly instructive way. Security Innovation offers a Cyber Range with a gaming-like approach to demonstrate mastery of security topics in real-world situations. Research shows that the Cyber Range is most effective at reinforcing concepts than alternatives.

Cyber Range is useful for measuring retention and the ability to apply concepts objectively that are relevant to specific job roles. Cyber Range is an unrivaled training approach that accurately measures engagement and builds confidence.

Features and benefits of Cyber Range:

- Monitor individual and group reports to track progress.
- Minimize time required to master security topics. Keep change agents on the bench.
- Measure outcomes of training against other job roles and industries.
- Fill skills gaps more rapidly while reducing training costs.
- Build confidence in a team's ability to deploy technology safely.

"You can't mitigate security threats until you really engage your team in training that grabs attention, motivates performance and measures success. Our Cyber Range is the best training method because it accomplishes all 3 objectives in the context of a learner's job role. The scenarios are realistic and real world."

ED ADAMS, CEO, SKILLSOFT PARTNER SECURITY INNOVATION

SUMMARY

Creating a more resilient security landscape begins with embracing basic principles. Think of basic principles as the foundation of our model. They reflect objectives for creating a more secure organization.

Every organization is on a unique path towards building a resilient security model that is rooted in a culture of learning. Is your organization prepared to do the following?

- Reset priorities for security in Dev and DevOps.
- Consistently practice basic security principles.
- Measure proficiency at identifying TTP.
- Build a security champions program across job roles.
- Build a security model tailored to your organization's exposures.
- Apply prevention lessons we learned from COVID-19.
- Compare your organization's proficiency to other industries.

Do what you can, before it's too late.

For more information on building security skills visit Skillsoft Percipio technology learning solutions at **www.skillsoft.com/techdev**

ABOUT SKILLSOFT

Skillsoft delivers online learning, training, and talent solutions to help organizations unleash their edge. Leveraging immersive, engaging content, Skillsoft enables organizations to unlock the potential in their best assets – their people – and build teams with the skills they need for success. Empowering 36 million learners and counting, Skillsoft democratizes learning through an intelligent learning experience and a customized, learner-centric approach to skills development with resources for Leadership, Technology and Development, and Compliance.

Skillsoft and SumTotal are partners to thousands of leading global organizations, including many Fortune 500 companies. The company features three award-winning systems that support learning, performance and success: Skillsoft learning content, the Percipio intelligent learning experience platform, and the SumTotal suite for Talent Development, which offers measurable impact across the entire employee lifecycle.

Learn more at **www.skillsoft.com**.

linkedin.com/company/skillsoft
facebook.com/skillsoft
twitter.com/skillsoft
skillsoft.com

US 866-757-3177
EMEA +44 (0)1276 401994
ASIA +65 6866 3789 (Singapore)
AU +61 2 8067 8663

FR +33 (0)1 83 64 04 10
DE +49 211 5407 0191
IN +91 (0) 40 6695 0000
NZ +64 (0)21 655032

skillsoft