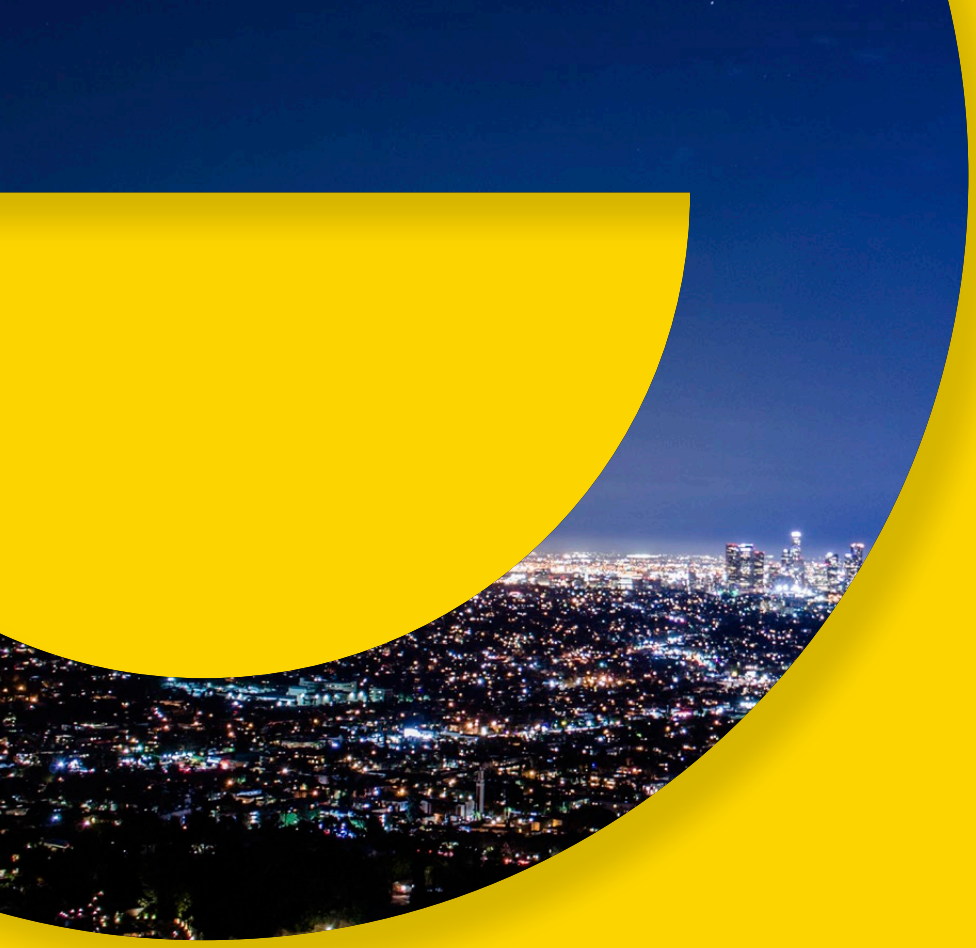


SUGARSHOT

You are going to get Hacked

WHAT TO DO & HOW TO STOP IT

A Must Read for Every Business Leader

BY SCOTT SPIRO

CONTENTS

Introduction — 3

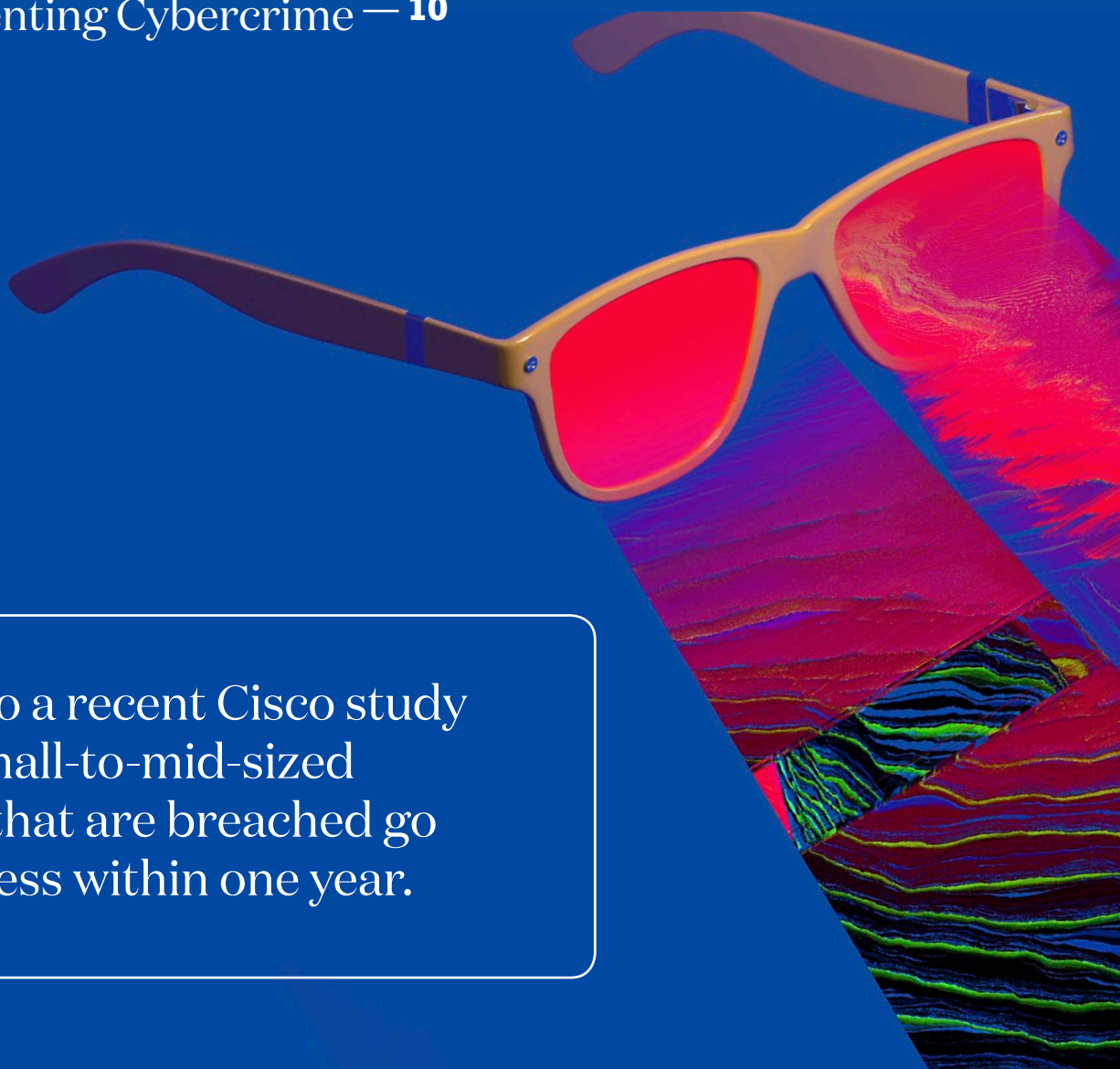
The rise of Cybercrime — 4

Understanding Cybercrime — 5

Changing the culture of how we do business — 6

The first critical steps to take after a hack — 7

Steps to preventing Cybercrime — 10



> According to a recent Cisco study 60% of all small-to-mid-sized businesses that are breached go out of business within one year.

INTRODUCTION

THERE ARE FEW ILLEGAL ACTIVITIES ON THE RISE AS RAPIDLY AS CYBERCRIME IS.

Now, more than ever, businesses are more prone to security breaches, and less prepared. We have become technology dependent, and as teams grow, so do our infrastructure and software solutions. With more potential areas open to exposure, cyber breaches in small to medium businesses are at an all-time high and yet, over 50% of surveyed businesses admit that their security measures, systems and processes are not adequate.

THE RISE OF CYBERCRIME

According to Key findings from the Global State of Information Security® Survey 2017, which was conducted by PricewaterhouseCoopers, there was a 38% increase in the instances of phishing scams and other cyber-security incidents. These breaches are not isolated to computer systems alone, either. Today's cybercriminal will also hack cloud architecture and even mobile devices. In fact, 28%+ of the incidents in the survey were on mobile technology. Ultimately, these are the reasons why 55% of individuals, businesses, and other entities now collaborate with cybersecurity specialists to better ensure their safety.

FOR MANY COMPANIES WITHOUT DEDICATED SECURITY DEPARTMENTS, IT'S NOT A MATTER OF IF, BUT WHEN. THE SIMPLE FACT IS: YOU ARE GOING TO GET HACKED.

Depending on the intent of the hacker, a business may have their data stolen, significant downtime to deal with or complete system destruction. Cybercrime is not just reserved for big businesses either. organizations of every size are vulnerable to attack, because there is one thing that we all have, that criminals want —your data. They are willing to work relentlessly, 24/7, using technology that finds the weakness in your security to expose it via a breach.

UNDERSTANDING CYBERCRIME

There is good news. Thankfully, significant strides have been taken toward effective prevention of breaches and the disruption that ensues from one. There's also steps you can take even after a breach has occurred to minimize the damage and protect your data.

As a business owner or decision maker, the steps you take after you discover you've been hacked are critical. Some breaches are immediately detectable.

For instance, Ransomware is the best-known example of this type of breach. This crime involves file encryption and then there is a demand for ransom that follows—pay the ransom and they will decrypt your files and release your information back to you. If the ransom isn't paid in time, you may lose your files completely. Even in some cases, you may pay ransom, but still not get the files back.

Other breaches are slow and use spyware, making it so you don't realize they've been stealing your business data over an extended period. Most businesses only notice this kind of attack after 200 days, according to the FBI in LA. In addition to this, there is an estimated $4.6 million per month stolen from cybercrime.

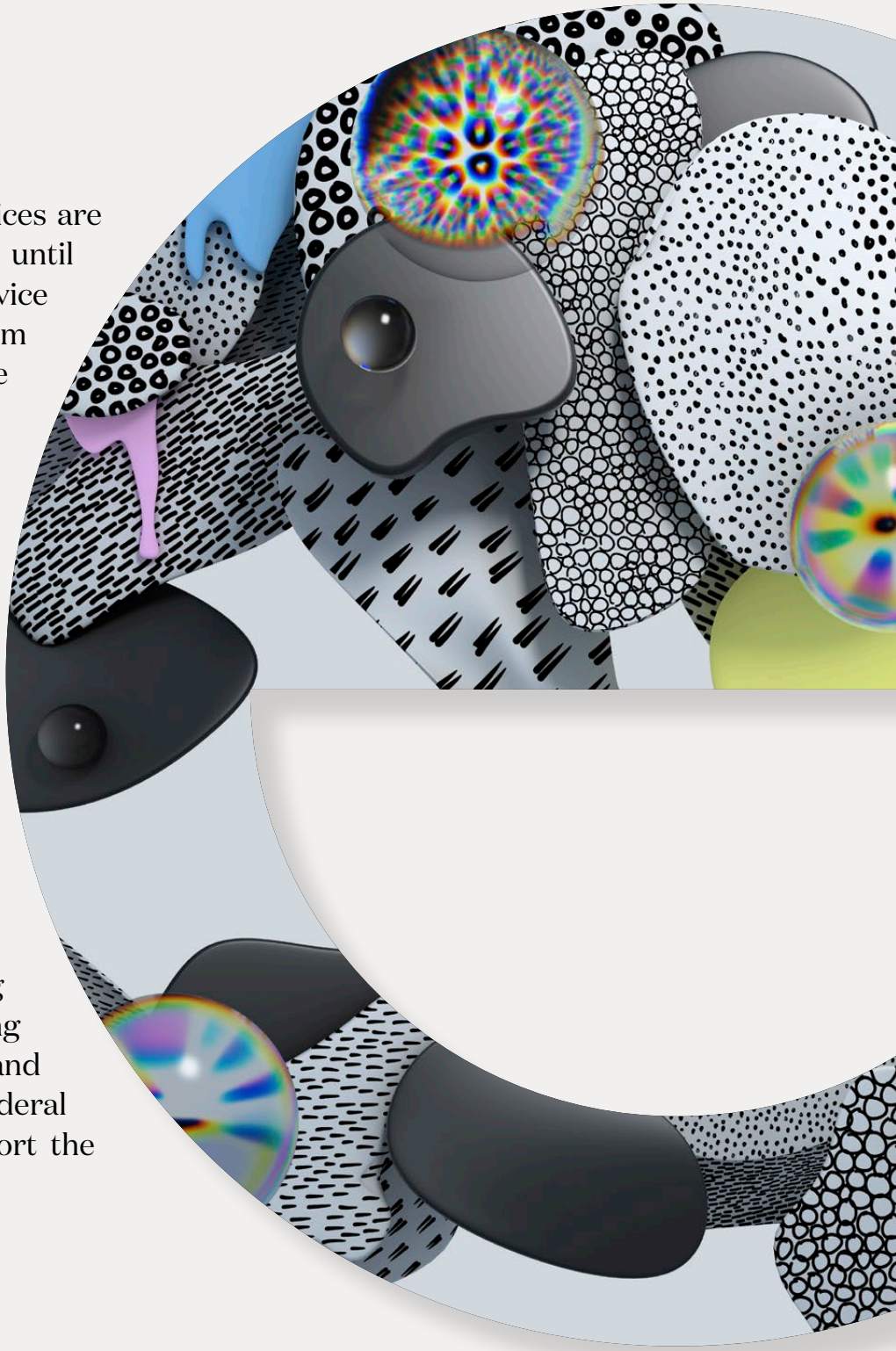
CHANGING THE CULTURE OF HOW WE DO BUSINESS

It can be challenging to grasp the severity of a security breach, but it is a crime—always. The one thing you do not want to do is assume your business won't become victim to one. The odds are against you, and the threat is serious enough that the federal government has even released guidelines to help you recover from an attack.

But what also needs to change in the general business community is the perception and approach to security. We are entering an era of business where security is no longer a 'nice to have' part to your business. It must become essential, considered, planned and executed to the highest level. The potential cost to businesses from downtime, data-loss, intellectual property theft and un-recoverable information is too great to avoid.

Defending yourself against cybercrime is nearly impossible to do alone, especially if you rely on any technology to conduct your business. The perpetrators are professionals and they are hard to counteract with amateur efforts. But there are some quick lessons you can learn to guard yourself against, and minimize damage in the event of, an attack.

THE FIRST CRITICAL STEPS TO TAKE AFTER A HACK



1. STOP USING EVERY DEVICE THAT IS INFECTED.

If you are not certain which devices are impacted, stop using all of them until you can connect with your IT service provider. Connect with them immediately, as well, because communication with them is imperative from this point on. Ideally your IT partnership will already have the right systems in place for helping to determine which devices—both on your business's site and through BYOD or COPE plans—are infected.

2. NOTIFY RELEVANT PARTIES OF BREACH.

Getting the word out that your business has been compromised is necessary. This requires letting all employees know, alerting potentially-impacted clients, and contacting any media outlets or federal entities that require you to report the hack for your specific business.

3. RESET ALL PASSWORDS.

The new "norm" for passwords is to change them periodically for routine maintenance and enhanced security. This is logical with the 10 million user password hacks that occur daily. However, Microsoft has recently changed their password security recommendations to be even stronger. These steps include:

- MAINTAIN 8 CHARACTERS — LONGER IS NOT NECESSARY
- ELIMINATE THE CHARACTER COMPOSITION REQUIREMENTS
- EDUCATE YOUR USERS REGARDING NOT REUSING THEIR PASSWORD FOR NON-NETWORK RELATED PURPOSES
- BAN COMMON WORDS - TO KEEP VULNERABLE PASSWORDS OUT OF THE SYSTEM
- ELIMINATE THE MANDATORY PASSWORD CHANGE REQUIREMENT
- FORCE REGISTRATION FOR MULTI-FACTOR AUTHENTICATION

4. BEGIN A FORENSICS EVALUATION.

This is imperative. Start by asking: what was the reason that someone wanted to gain access to the system? Was it for intellectual property, client data, etc.? Your business was targeted and it is important to know why, exactly. This information is highly valuable to federal cybercrime divisions such as what are in the FBI, IRS, and Department of Homeland Security. If there is a trend showing on the vertical (similar businesses) more can be done to pinpoint, identify, and hopefully prevent your business from being attacked again. Plus, similar businesses can take proactive steps to not become the next target. This type of cooperative teamwork is how local and federal authorities can work together to help businesses and make cybercriminals' jobs' much more difficult.

IT CAN MAKE SENSE TO HIRE AN EXTERNAL PARTY TO HELP WITH THIS EVALUATION BUT THIRD PARTY QUALIFIED EXAMINERS NECESSARY TO DO A THOROUGH, FULL-FORENSICS INVESTIGATION ARE HIGHLY COSTLY. YOU WILL SAVE CONSIDERABLE AMOUNTS OF MONEY BY PROACTIVELY INVESTING IN THE TECHNOLOGY AND USER TRAINING TO HELP WARD OFF CYBER-ATTACKS FROM INFILTRATING YOUR BUSINESS

5. PERFORM AN UPDATED VIRUS SCAN ON YOUR ENTIRE SYSTEM.

Most major tech companies will have ways to get your account back up and running and with minimal data loss if you invested in the proper backup system technologies. However, this can be in vain if you don't remove every single virus on the system. Failure to remove all threats can mean that you restore your system only to find that that it goes down again the next day.

6. DETERMINE THE NEED FOR CREDIT MONITORING.

Whether the hack was on you personally, or a business hack in which large amounts of Personally Private Information (PPI) was retrieved, you will want to have credit monitoring in place for impacted victims. Identity theft is a serious crime, and according to the 2017 Identity Fraud Study released by Javelin Strategy & Research, $16 billion was stolen from 15.4 million US consumers in 2016, compared with $15.3 billion and 13.1 million victims a year earlier. In the past six years, identity thieves have stolen over $107 billion. These numbers show why criminals are incentivized to gain access to your data.

7. REMAIN IN COMMUNICATION, AS DEEMED NECESSARY.

Communication is critical after a hack between your IT provider, impacted business, and the appropriate authorities.

The communication required includes:

i. Affected businesses coming forth with any and all things they recognize are not operating properly;

ii. The IT company explaining what they are doing, and why, while also giving guidance to smarter practices;

iii. The IT company and business both communicating with authorities, as needed, to help them gain the valuable data and information that can help them solve cybercrimes.

SUGARSHOT TIP

IN A RECENT STUDY, CISCO ESTIMATES THAT 60% OF ALL SMALL-TO-MID-SIZED BUSINESSES THAT ARE BREACHED GO OUT OF BUSINESS WITHIN ONE YEAR. BEING PROACTIVE AND NOT TAKING YOUR TECHNOLOGY'S SECURITY FOR GRANTED WILL HELP YOU PREVENT BECOMING A STATISTIC.

STEPS TO PREVENTING CYBER CRIME

Businesses have more control over maintaining their business assets and data than they often realize. Businesses should embrace the active role they can take in ensuring that they do not become the victim of an attack. There are many things that can be done, which will help strengthen their defenses.

1. ALL EMPLOYEES MUST BE TRAINED.

You can have the most sophisticated technology in place to protect your business system(s) from a breach, but if your employees do not understand their role, any system you may have is rendered less effective. Think about a security system for your home. We put it in place to protect our loved ones and our possessions from a criminal entering our home. If that criminal comes knocking and your child answers, the entire security system that is in place has just been bypassed. The same is true of your business, and the way in which your employees adhere to security guidelines and safe practices.

2. TEACH EMPLOYEES ABOUT THE WAYS THAT CRIMINALS GAIN ACCESS TO INFORMATION.

Social engineering is a way of tricking employees to give a criminal access to certain targeted information. This crime can either take place through email correspondence, or in some cases, through bold criminals who will walk into a business pretending to be a "new employee" of a service your business already uses. You need procedures in place for verification and identification. An effective way to ensure that employees are always engaged in safe practices is to do training exercises via anonymous email blasts to see if the team responds correctly.

3. BE DILIGENT IN ENSURING YOUR TECHNOLOGY IS AS PROTECTED AS POSSIBLE.

Patch updates and systems checks are necessary functions of any IT department that your business employs. There should never be delays to getting these updates done, because in those gaps there is a great potential for a breach. When it comes to your business' technology, having a partnership with an outside IT firm is the best way to ensure that everything that should be done is getting done.

4. TALK ABOUT SECURITY

Making security an important discussion in your business is the first step to highlighting its importance and getting everyone on the same page. All cybercrime prevention for businesses is a joint effort of sound leadership within the organization and the vested interest of employees. Through gaining the cooperation of the leadership and decision makers, you can create unity within an organization so everyone recognizes why they should be on board with newly-implemented policies and procedures to do their jobs in today's world.

5. FIND THE RIGHT PARTNER

Finally. defending yourself against cybercrime is nearly impossible to do alone, especially if you rely on any technology to conduct your business. The perpetrators are professionals and they are hard to counteract with amateur efforts. Find the right IT partner for you, who doesn't just help manage and procure your IT equipment, but proactively plans and initiates conversations s around security. With the right partner, you'll feel safer, and be safer from attacks in the future.


TECHNOLOGY.
DIFFERENTLY.

Technology. Differently.

—

Designed in Los Angeles, CA

SUGARSHOT

WWW.SUGARSHOT.IO
HI@SUGARSHOT.IO
(310) 641-6551
5777 W. CENTURY BLVD., SUITE 1500 LA, CA 90045

HEY YOU. IF YOU CAN READ THIS, WELL DONE - YOU GET FREE CANDY.
EMAIL FREECANDY@SUGARSHOT.IO WITH YOUR NAME AND ADDRESS.