

the
GORILLA
GUIDE[®] to...



Navigating the Security Landscape

How To Stay Vigilant, Current,
and Educated

S. MICHAEL BENSON

Navigating the Security Landscape

By S. Michael Benson

TABLE OF CONTENTS

Introduction.....	4
Current State of Security.....	5
The Current Landscape.....	11
What You Need to Know	14
Beyond the 'Now': The Long-Term Outlook.....	16
Stay One Step Ahead.....	17

Copyright © 2022 by ActualTech Media

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

ActualTech Media

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829
www.actualtechmedia.com

Publisher's Acknowledgements

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

PARTNER AND VP OF CONTENT

James Green

ABOUT THE AUTHOR

S. Michael (Mike) Benson is the owner and principal architect for Emprize IT Consulting. He spent 30 years at IBM as an executive IT architect in technical sales where he led client workshops and studies across a wide variety of technical topics before starting Emprize. Mike has been a frequent conference speaker and has published many technical articles and whitepapers.

Introduction



Welcome to this Gorilla Guide® To... Navigating the Security Landscape, Foundation Edition. Security is a topic that generates fear in the hearts of IT professionals. No one wants to be in the headlines for the next major security breach.

In this book you'll find a review of the major focus areas dominating IT security, now and into the future. Included is a set of actions that you can take to tighten your security environment and some long-term direction for security technology in general.

Hopefully, this Gorilla Guide will help you replace fear with knowledge as you learn where cybercriminals are focusing their effort and how you can prevent them from being successful in your organization. Are you up for the challenge? Let's get started!

Security has become a never-ending battle as cybercriminals continually hone their skills and attack with increasing sophistication. Security technologists respond as quickly as possible to reduce attack surfaces and close down vulnerabilities, trying to stay ahead of the hackers. It's like a marathon consisting of short-term sprints to respond to the next threat.

Business executives rate security as an issue that keeps them awake at night. No one wants to be in the headlines as the target of a security breach. A recent IBM and Ponemon study showed that security breaches cost companies an average of \$3.86 million. Not only is there a direct financial impact,

but indirect harm often results, as well, through damage to reputation and regulatory fines.

It's no wonder that companies and government agencies are investing in tools to help detect potential breaches before they happen, or at least before sensitive information is compromised. While there's not yet a silver bullet to render would-be hackers impotent, advances in artificial intelligence (AI) will likely level the playing field and should give businesses the upper hand.

Current State of Security



We are in a time of new opportunities for cybercriminals as the global COVID-19 pandemic pushed many businesses to change the ways they use technology. Companies were so focused on preserving income and keeping their newly remote workforce productive that security considerations often took a back seat.

But cybercriminals haven't taken a break during the pandemic. Instead, they've leveraged the resulting disruption to find new attack methods and double down on existing ones. Unfortunately, many companies were not prepared for disrupting events like the pandemic and are only reacting rather than staying ahead of the hackers. We haven't seen the full impact of the pandemic on businesses yet, but it's likely many breaches will be reported in the coming years.

Here's a brief description of five key security areas that will be particularly challenging in the near- and long-term.

RANSOMWARE

Ransomware continues to be a thorny issue for organizations, and has quickly become the No. 1 issue in the realm of IT security. Not only have the number of attacks multiplied, but the ransom demands have also increased so that over more than one-third of the hostage organizations were forced to pay over \$1 million, with annual total cost being in the billions.

One of the newest and most problematic ransomware attacks, labeled *Sodinokibi*, was seen in roughly a third of the attacks by the IBM Security X-Force Incident Response team. The ransomware is typically downloaded through an email phishing attack, but what makes it so dangerous is that it is hard for antivirus tools to detect. The downloaded zip file contains an obfuscated JavaScript file that executes when opened.

Ransomware attacks have typically been extortion attempts to make a business pay to get its data released through decryption. Ransom demands are increasing exponentially; for some large enterprises the amount exceeds \$40 million.

A newer trend in ransomware attacks involves the possible release of sensitive data instead of just its loss. In these newer attacks, the attacker often makes a copy of the data and threatens to release sensitive information that could be used in second order attacks such as identity theft. This may be a reason why cybercriminals have raised ransom demands.

REMOTE WORKFORCE

With many governments requiring people shelter in place to slow the spread of the coronavirus, businesses have had to quickly ramp up a work-from-home infrastructure that was never designed to handle the volume and type of work now required. **Figure 1** shows how the percentage of U.S. workers now working five or more days a week from home has grown.

This has created fertile ground for cybercriminals to probe and exploit since many people working from home are using their personal equipment and Wi-Fi to access company applications and data. IBM Security Systems noted that spam increased by 5,000% at the beginning of the shelter-in-place

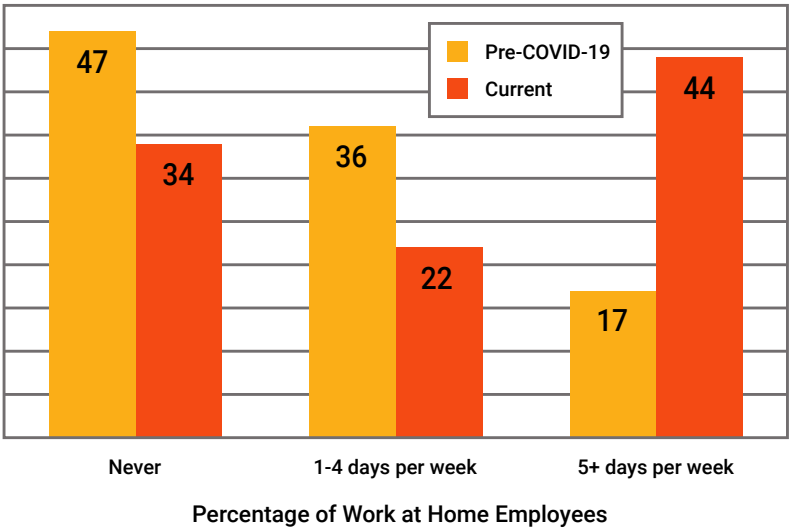


Figure 1: The effect of COVID-19 on the number of employees working from home

directives. No doubt much of this spam contained malware attempting to compromise personal systems attached to company infrastructure.

INTERNET OF THINGS (IoT) SECURITY

As intelligent devices proliferate in the marketplace, they create a much larger attack surface, bringing increased vulnerabilities that cybercriminals were quick to recognize. Every smart device is connected to the Internet through a unique IP address that hackers can use to invade home and business networks.

Network-attached smart devices have become big business, with many homeowners using them to control different home functions. However, security hasn't been a priority for many smart device manufacturers and cybercriminals know this. Hardcoded or guessable passwords and weak or nonexistent network security are the two largest areas of concern.

As intelligent devices proliferate in the marketplace, they create a much larger attack surface, bringing increased vulnerability that cybercriminals were quick to recognize.

There's hope on the horizon, as the U.S. Congress passed a law addressing IoT cybersecurity in the government with enforceable standards. This is a good first step, but must be expanded to consumer devices.

SOFTWARE VENDOR BREACH

The SolarWinds debacle is an example of how cybercriminals were able to extend their reach by attacking a software vendor. Intruders injected malware into the software compilation process, secretly inserting backdoor software into the SolarWinds Orion infrastructure tool, which was then released to companies and government agencies that licensed Orion. Through the installed backdoor, cybercriminals were able to move laterally across internal networks to access sensitive data.

By breaching the SolarWinds network management tool, the perpetrators were able to distribute their malware to thousands of companies and over a hundred government agencies through the normal software patching process. The effects are staggering, and still being assessed.

SKILLS SHORTAGE

Recent studies have shown that over half of worldwide cybersecurity positions are currently open. Demand is increasing at a rate faster than people are being trained and this has caused security risks for many companies that can't find skilled workers. The risks include overworked and undertrained

cybersecurity staff. **Figure 2** shows how the cybersecurity skills deficit has grown over the past five years.

The development of newer cybersecurity automation, which employs AI and robotic processes to detect and remediate security threats, brings hope that this will be less of an issue in the coming years. These tools are now mainstream and have helped alleviate some of the skills shortages for the companies using them.

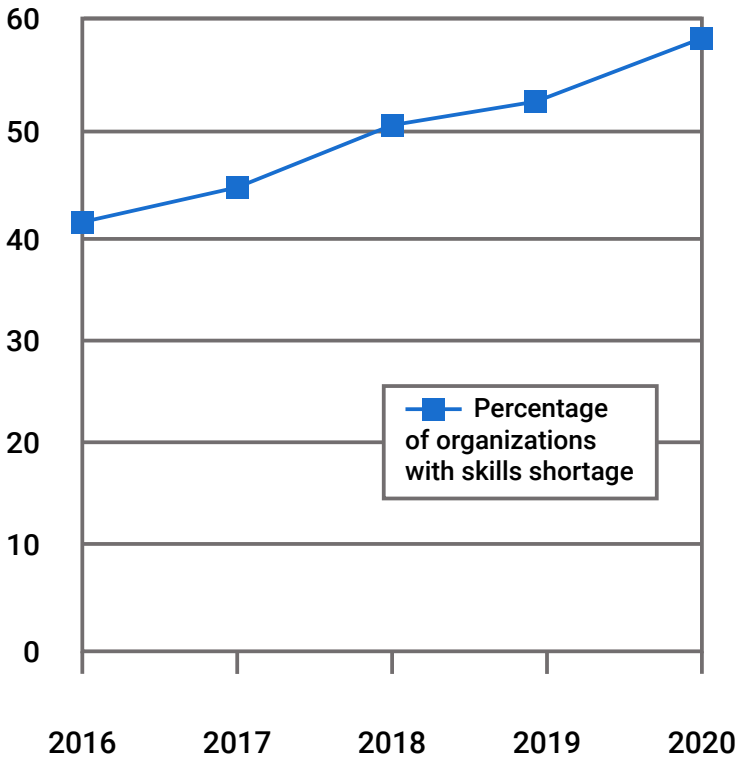


Figure 2: Increasing cybersecurity skills shortages

The Current Landscape



As new technologies continue to be rolled out and the pandemic continues its onslaught, cybercriminals will be relentless in finding new attack vectors with increasing sophistication.

Here are five key areas seeing increased focus:

TELEMEDICINE

The use of consumer-grade video conferencing services for sensitive telemedicine visits provides a target for cybercriminals. More health care providers will begin to use enterprise-grade conferencing software with stronger security controls in place to thwart would-be hackers from acquiring sensitive personal information.

Expect cybercriminals to continue probing for vulnerabilities in the health care infrastructure as more online records and data sharing occurs. DarkOwl researchers noted a 144% increase in telehealth keywords on the dark web, signifying a growing interest in targeting health care providers.

5G NETWORKS

As cybercriminals become more familiar with 5G engineering, more vulnerabilities will be exposed. The biggest concern is that 5G requires significantly more network devices, since its range is far shorter than its predecessors'. More devices mean more attack surfaces to be targeted.

5G isn't just for cellular telephone communication. It's a new mobile network architecture that has applications in everything from autonomous vehicles to remote surgery to all kinds of consumer and industrial IoT devices. Cybersecurity compromises across the spectrum of 5G-enabled devices could be catastrophic. Fortunately, standards bodies such as 3GPP and NIST have developed 5G security frameworks that are becoming widely implemented.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Even as more security vendors are integrating AI and machine learning (ML) into their threat detection and mitigation processes, cybercriminals are also beginning to use AI to find unique vulnerabilities that can be exploited.

Next-generation firewalls use ML to discover and prevent cybersecurity attacks from breaching internal networks. By learning to recognize anomalies, these devices can even prevent zero-day attacks from being successful. ML is also being used by network management tools to analyze patterns and recognize would-be attackers before they get a foot in the door.



Cybercriminals are also beginning to use ML to develop new attacks that are harder to detect. One such attack uses AI-enabled voice fraud to simulate company executives requesting funds transfers to the hacker's private accounts.

Adapting Infrastructure

A recent survey conducted by Navisite showed that 83% of respondents plan to continue work-from-home policies after pandemic restrictions are lifted. Desktop as a Service and Workplace as a Service will see growth as businesses adapt infrastructure to increased work-from-home demands with stronger built-in security.



SUPPLY CHAIN TARGETS

With the SolarWinds hack clearly affecting thousands of companies as well as many government agencies, cybercriminals have realized they can cast a much wider net by attacking supply chain targets and letting normal distribution channels spread their malware.

Though the current belief is that the hack was performed by a foreign government, it's virtually certain that independent cybercriminals are studying how it became so successful and will attempt to duplicate it.

WORK-FROM-HOME SOLUTIONS

With continued work-from-home solutions being used by companies to maintain employee productivity while the COVID-19 virus is being fought, cybercriminals will find more vulnerabilities to exploit. VPNs are a minimum necessity, but

many are inadequate to protect companies from advanced threats. In addition, home Wi-Fi networks and personal devices can be compromised, leading to a direct path over the VPN to corporate networks and data.

What You Need to Know



You don't have to sit by and watch company after company struggle with cybersecurity breaches. Here are four actions you can take to reduce your risk of being the next company in the headlines.

STAY VIGILANT

Cybercriminals don't sit still. They're constantly looking for new ways to breach existing security systems through zero-day attacks. You have to run software that constantly assesses possible threats as they happen so you can stay in front of potential hacks.

For many companies this means acquiring state-of-the-art security software that uses AI and ML to stay ahead of cybercriminals. Security protection is a 24/7 activity.

STAY CURRENT

Make sure you're up-to-date with security patches for all of your systems and applications. One of the most common vectors of injection is out-of-date software with security vulnerabilities. Kaspersky Lab estimates that 98% of the

disastrous Wannacry ransomware infections were running on outdated and unpatched Windows 7 systems.

Subscribe to a signature-based security service that will continually alert you to new attack methods. Augment this with behavior-based services to detect anomalies using ML.

STAY EDUCATED

Cybercriminals usually find a way into corporate networks through unsuspecting or naive employees who are unaware of hacking techniques. Many companies generate internal phishing emails to test employees and reinforce proper handling of emails with attachments.

Providing education on how cybercriminals trick users will go a long way toward thwarting attempted breaches. This can be handled internally if you have the staff, or via external education with a recognized security training firm if you don't.

STAY STAFFED

Not having enough skilled security staff is a major risk. People are often stretched too thin and can't possibly handle the quantity of incoming threat assessments. Because of the worldwide skills shortage, the best way to beef up your staff is to retrain existing employees.

You'll have trouble finding experienced people to hire since most have already been scooped up by other companies. If you do find someone with skills, you'll have to pay top dollar for their services and may end up in a bidding war.

Beyond the 'Now': The Long-Term Outlook

Cybersecurity will increasingly become a primary focus of IT organizations and may cause a regression in development agility as companies struggle to protect their critical assets as they work to provide competitive goods and services. Two specific areas that have major security implications in the future are AI and a fractured Internet.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

The role of AI in cybersecurity protection will expand to a level where fewer cybersecurity professionals are required, since AI automation will neutralize attacks before they can do damage. This is probably still a couple of years away, but tools are already becoming more sophisticated and are able to provide some services in a limited capacity.

In addition, ML will enable security processes to anticipate upcoming threats before they occur, so you can be more proactive. As with any ML, it takes time to develop the model and train the data, but this will only get better with time.

FRACTURED INTERNET

More nation-states are looking at using a weaponized Internet to carry out global attacks that provide them with a global advantage. If these activities continue, we may need to

rethink how the Internet works and shut down connectivity to rogue actors. Of course, this is antithetical to the purpose of the Internet, but as a security precaution, it may become necessary.

Already some nations are trying to censor information flowing across the Internet as it enters and leaves their countries. Expect this to increase as disinformation and fake news continue to be generated by those trying to disrupt governments and businesses.

Stay One Step Ahead



The current Internet situation has often been called the “Wild West,” as there’s very little law enforcement or protection. Technology has outstripped our ability to make and enforce new laws to address cybersecurity. Hopefully, our laws will catch up before the next big technology change and we’ll be able to apply law and order to the infrastructure.

In this Gorilla Guide you’ve learned about the major trends impacting the IT security landscape at present and what we could be seeing in the future.

Cybersecurity professionals must continue to stay one step ahead of cybercriminals. Eventually, they’ll be replaced entirely by machines that protect other machines, removing the human element altogether. Until then, there are no cybersecurity silver bullets—only diligence and hard work to stay ahead of the cybercriminals.

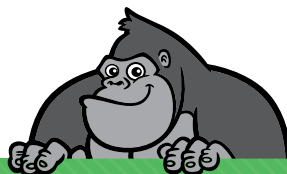
About ActualTech Media



ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit <https://www.gorilla.guide/custom-solutions/>