



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Crane, Casey

“The Top Cyber Security Trends in 2019 (and What to Expect in 2020)”

Thesslstore.com

The SSL Store

23 August 2019

URL: <https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/>

Accessed: 15 August 2019

Synopsis: A look at the emerging trends in cyber security this year and a sneak peak at what to expect in the coming year Cyber security is a hot topic for organizations and businesses of all sizes across every industry. Of course, every company has different priorities and insights, so the lists of cyber security trends for 2019 and 2020 you'll see around the internet vary quite a bit depending on your source. However, many of the lists do at least share some common characteristics. And as cyber attacks continue to increase in frequency year over year, they all serve to underscore the importance and need for better cyber security defenses. Some of the current trends in IT security relate to the types of attacks, methods of prevention, and industries that are being targeted. Others are about finding new methods and technologies to: Reduce cyber security vulnerabilities; Better secure networks; Use automation and other processes to make takes more efficient and cost-effective; Increase data privacy and compliance; and Improve the collection and analysis of data. So, what has made our list of the top cyber security trends in 2019, and where do we expect to see these cyber security trends go in 2020?

Let's hash it out.

The Top Cyber Security Trends in 2019 (and What to Expect in 2020) - Hashed Out by The SSL Store™

Author

A look at the emerging trends in cyber security this year and a sneak peak at what to expect in the coming year

Cyber security is a hot topic for organizations and businesses of all sizes across every industry. Of course, every company has different priorities and insights, so the lists of cyber security trends for 2019 and 2020 you'll see around the internet vary quite a bit depending on your source. However, many of the lists do at least share some common characteristics. And as cyber attacks continue to increase in frequency year over year, they all serve to underscore the importance and need for better cyber security defenses.

Some of the current trends in IT security relate to the types of attacks, methods of prevention, and industries that are being targeted. Others are about finding new methods and technologies to:

- Reduce cyber security vulnerabilities;
- Better secure networks;
- Use automation and other processes to make takes more efficient and cost-effective;
- Increase data privacy and compliance; and
- Improve the collection and analysis of data.

So, what has made our list of the top cyber security trends in 2019, and where do we expect to see these cyber security trends go in 2020?

Let's hash it out.

The top cyber security trends of 2019

We've put together a list of what we believe are the trends in IT security that are dominating the industry this year. The trends we've listed below are a combination of both factors we believe impact both cyber security defenders and cybercriminals alike.

Multi factor authentication (MFA) has been an ongoing trend for a few years now. MFA, sometimes known as two-factor authentication (2FA), requires a set of factors to access restricted data — something you know (such as a password or pass phrase), something you have (such as a security token of some kind), and something you are (biometrics such as a retinal scan or fingerprint).

Cyber security trend #1: The phishing landscape is changing, though email still ranks as the biggest of those threats

It should come as no surprise that phishing would make our list of the top cyber security trends. Phishing has been a staple of cyber security trends lists for a while, and it doesn't

appear to be going anywhere any time soon. [Verizon's 2019 Data Breach Investigations Report](#) (DBIR) reports that 32% of confirmed data breaches boiled down to phishing, and 78% of cyber-espionage incidents involved phishing.

But phishing nowadays isn't just about emails alone — though email is still an incredibly popular attack vector. Cybercriminals are also using a variety of attack vectors to reach and trick their intended victims into performing an action — such as giving up personal information, login credentials, or even sending money. Increasingly, phishing nowadays involves general SMS texting attacks (“smishing”) everything from [communications on social media platforms such as LinkedIn](#) to phishing sites to even phone calls with a live person (“vishing”). You know those fake IRS phone calls, Social Security scams, and people pretending to be Microsoft? Yeah, those are just a couple of examples of vishing.

Cyber security trend #2: Increasing use of mobile as an attack vector

Considering that nearly everyone nowadays has a mobile device in their pocket, it really comes as no surprise that mobile made its way near the top on our list of cyber security trends for 2019. After all, being mobile makes life more convenient. You can use your mobile devices for handling everything from personal and business communications to banking or even booking a flight or hotel. There are apps for literally every aspect of your life. Bored? Play a game app. Want music? Turn on a music app. Need to lose weight? There's an app you can download for that, too.

But all of this convenience doesn't come without risk for end users and companies alike — particularly as more people use their personal and work devices interchangeably for personal and businesses purposes. This practice spells out concerns for businesses. Research from the [RSA's 2019 Current State of Cybercrime](#) whitepaper shows that “70% of fraudulent transactions originated in the mobile channel in 2018.” Furthermore, “fraud from mobile apps has increased 680 percent since 2015,” making it a huge channel of opportunity for cybercrime.

Cyber security trend #3: Targeting of local governments and enterprises via ransomware attacks

So long as you haven't been living under a rock the past few years, then it's likely you've seen that the rates of ransomware attacks against consumers are down this year. However, the same can't be said for enterprises. Ransomware are on the rise for enterprises with [research from Malwarebytes](#) reporting an increase of 195% from Q4 2018 to Q1 2019, as well as a year-over-year increase of 500% in ransomware detections by businesses in Q1 2018 to Q1 2019.

Even governments aren't safe from ransomware. Research from [Recorded Future](#), a threat intelligence firm that has catalogued nearly 170 ransomware attacks affecting state and local governments since 2013, shows that ransomware attacks against these government branches are on the rise. Their data reports that there were 53 ransomware attacks against state and local governments in 2018, and that there were 21 reported attacks within the first four months of 2019. Furthermore, “the numbers for 2018 and 2019 may go up, as not all ransomware attacks against state and local governments are reported immediately.”

For example:

- [20 cities in Texas were hit by coordinated ransomware attacks](#).
- [Three Florida cities](#) were targeted by ransomware attacks, and at least two paid the demanded ransoms to unlock their data.
- The city of [Baltimore, Maryland sustained two ransomware attacks](#) in 14 months.
- The city of Atlanta, Georgia sustained a major ransomware attack in March 2018, which left the city crippled and facing [upwards of \\$17 million](#) in costs relating to the attack. The [same attackers](#), two Iranian hackers, also targeted the city of Newark, New Jersey,

and others.

The list goes on and on — and that's just U.S. cities. This list doesn't even contain information relating to other major cities or government offices across the world that have been the victims of ransomware attacks.

[Research](#) from Coveware, a security firm that specializes in ransomware incidents, indicates that while the public sector represents only 3% of ransomware attack victims in Q2 2019, the public-sector ransomware victims who chose to pay the ransoms paid nearly 10 times as much money, on average, as their private-sector counterparts. This could be, in part, due to a lack of cyber security awareness. However, regardless of the cause, governments paying *any* ransom poses a significant concern because it reinforces the notion that performing ransomware attacks against governments is a profitable venture and will only serve to encourage them to conduct more attacks.

Cyber security trend #4: Increasing emphasis on data privacy, sovereignty, and compliance

Since the rollout of the European Union's General Data Protection Regulation (GDPR) in May 2018, states, countries, and industries alike around the world have begun taking harder looks at their existing data privacy-related regulations. The goal? To [develop, pass, and implement new regulations](#) that will ensure higher data security and privacy standards to better protect consumers (or citizens, depending on the specific example) and to punish those who fail to abide by them.

Data sovereignty and compliance, of course, come in different forms. Depending on the specific legislation, it can involve:

- Informing individuals about how their information will be used;
- Providing individuals with a way to disallow their information from being shared;
- Developing and implementing policies and procedures to become compliant; and
- Increasing the security of data and personal information through the use of encryption and other mechanisms.

However, there are also proposed regulations that approach the topic of data privacy from a different angle. In some cases, the emphasis is placed on creating encryption "backdoors" to make it easier for governments to access encrypted information in the name of justice and thwarting terrorism activities.



Manage Digital Certificates like a Boss

14 Certificate Management Best Practices to keep your organization running, secure and fully-compliant.

Cyber security trend #5: Increasing investments in cyber security automation

Here we are — the final stop on our list of the top cyber security trends for 2019: automation.

Automation is a very important advantage in cyber security that has been gaining a foothold in the industry. A recent [Ponemon Institute survey](#) of more than 1,400 IT and IT security practitioners shows that 79% of respondents either currently use (29%) automation tools and platforms within their organization or plan to use them (50%) within the next six months to three years.

Depending on the cyber security automation tools and platforms, they can help you perform many tasks, including:

- Collecting data about components of your information system that can be used to monitoring and analysis.
- Keeping track of all software and hardware assets within your organization.
- Keeping all of those physical and virtual assets patched and up to date.
- Performing vulnerability assessments to identify known or potential vulnerabilities.
- Increasing visibility and decreasing downtime with X.509 digital certificate discovery, renewals, installations, revocations, etc.

This movement towards the use of automation aims to reduce the burden on understaffed cyber security teams and increase efficiency. However, it's not a perfect solution on its own because automation tools require skilled and knowledgeable staff to operate them. This is a problem when you consider that the same Ponemon Institute survey results indicate that 56% of organizations report a “lack of in-house expertise” to support the adoption of automation.

Although we've listed automation on our 2019 list of cyber security trends, we expect that this is an ongoing trend that will continue well into next year and the years to follow as cyber security future trends.

Hey, don't go anywhere — we're not done quite yet. We've still got a few more insights to share about cyber security future trends for the coming year.

Cyber Security Trends 2020: What to Expect in the Coming Year

Some of the cyber security trends we mentioned for 2019 are likely to carry over into 2020. However, here are a few things we see in 2020:

Cyber security spending will continue to increase

Cyber security spending is on the rise. In fact, [data from IDC](#) shows that global spending on cyber security solutions such as hardware, software and services is anticipated to top \$103 billion this year alone. That's an estimated increase of 9.4% over 2018 — and they expect this rate of growth to continue for the next several years as industries and companies increasingly invest in security solutions. The U.S. is anticipated to be the largest individual market with spending forecasted to reach nearly \$45 billion by the end of the year.

According to IDC's March 2019 report:

“The three industries that will spend the most on security solutions in 2019 – banking, discrete manufacturing, and federal/central government – will invest more than \$30 billion combined. Three other industries (process manufacturing, professional services, and telecommunications) will each see spending greater than \$6.0 billion this year. The industries that will experience the fastest spending growth over the forecast period will be state/local government (11.9% CAGR), telecommunications (11.8% CAGR), and the resource industries (11.3% CAGR). This spending growth will make telecommunications the fourth largest industry for security spending in 2022 while state/local government will move into

the sixth position ahead of professional services.”

The growing impact of AI and ML on cyber security

Artificial intelligence and machine learning in cyber security are the second on our list of the cyber security trends for 2020 — and for good reason. As we shared in a previous article on [artificial intelligence in cyber security](#), machine learning and artificial intelligence are reinventing cyber security as a whole and are areas that are definitely worth exploring in the coming year. Data from a [Capgemini Research Institute survey](#) supports the idea that AI is vital to organizations’ cyber security defenses. Three-quarters of surveyed executives reported that AI helps their organizations respond more quickly to breaches, and 69% of the organizations reported that AI is necessary to respond to cyber attacks.

This could be in part because there are many advantages — as well as some disadvantages — to integrating artificial intelligence (AI) with your cyber security solutions:

- AI-based cyber security solutions are designed to work around the clock.
- AI can respond in milliseconds to cyber attacks that would take minutes, hours, days, or even months for humans to identify.
- AI simplifies the process of data collection and analysis.
- AI systems can be integrated for enhanced threat and malicious activity detection through predictive analytics.
- Greater access to valuable data helps cyber security professionals make better and more informed decisions.
- AI are helping create better and more accurate biometric-based login techniques.

However, AI isn’t perfect — there are some drawbacks to using the technology as well:

- AI technologies are being used by defenders and attackers alike — and they’re not one-size-fits-all solutions.
- AI-based solutions can be more expensive up front than traditional, non-AI cyber security solutions.
- AI-based solutions require more training for cyber security staff to effectively operate.

Regardless of the potential disadvantages, the market for artificial intelligence in cyber security is projected to reach 38.2 billion by 2026, according to data from a recent [Research and Markets report](#). That’s particularly significant considering that the company’s projections anticipate the industry reaching \$8.8 billion by the end of 2019.

Cyber attacks on utilities and public infrastructure will continue to increase

Let’s face it: Utilities are essential to a modern economy and also make excellent targets for cyber attacks. They provide critical infrastructure for millions of people and governments around the world, yet they often operate using old, outdated technology. But trying to upgrade their cyber defenses and fix cyber security flaws can lead to service interruptions and downtime. Add to that the fact that much of their infrastructure is controlled by private corporations — many of which are not prepared to deal with major cyber security threats — and you have a situation that is ripe for exploitation by hackers

Just look at the headlines this summer to see some recent examples of cyber attacks on utilities include the [recent attacks on U.S. utility companies](#) in July by suspected Chinese state hackers and the [ransomware attack that rocked City Power](#) in Johannesburg, South Africa.

When you think of emerging trends in cyber security for 2019 and 2020, what areas of cyber security immediately come to mind? As always, share your thoughts in the comments.