7 Cybersecurity Trends We're Likely to See in 2019

Devolutions

THIS ARTICLE WRITTEN BY PATRICK FOSTER, CONTENT WRITER FOR ECOMMERCE TIPS, IS PART OF OUR GUEST BLOG SERIES.

PLEASE CONTACT US IF YOU WOULD LIKE TO BE FEATURED ON OUR BLOG.

Check the calendar, open the nearest window: spring is in the air. That means, alongside your traditional spring clean, it's time once again to clear out your cyber clutter. Don't miss this fresh opportunity to actually change all those old and generic passwords you keep meaning (but forgetting) to do something about (stop putting it off!).

After all, it's pretty important in this increasingly-interconnected tech world that you keep your data and systems protected. Nefarious types are lurking everywhere, ready to drain your bank accounts and leak your private information to the world – and working as an MSP doesn't grant you special immunity. If anything, it paints a target on your back.

But what can we all expect when it comes to general cybersecurity as the year progresses? Are we in for any dramatic upheavals? Do we need to prepare for revised standards? Here are 7 cybersecurity trends we're likely to see more of in the coming months.

The cloud will continue to take over

The core appeal of cloud-based services — the hardware is handled for you, services can be accessed from (almost) anywhere, and they're updated in a timely fashion — makes them perfect for cybersecurity. Far better a strong remote system than a weak local one.

This year, more and more businesses will choose to outsource their cybersecurity needs instead of making ineffective attempts to implement custom in-house systems. Some will simply use login-style services, while others will take existing solutions and essentially plug them in: either way, they'll benefit from access to expert analysis and response procedures.

This will also clarify which cybersecurity businesses will rise to further prominence, and which ones will fall by the wayside. The top providers will rise hugely in popularity, while those that fail to impress will struggle to find anyone to give them the benefit of the doubt.

Cryptojacking will remain a stubborn problem

The immense rise in computers of many varieties being used to mine cryptocurrency did more than simply waste huge amounts of processing power and cause frustrating rises in the prices of consumer-targeted GPUs: it also led to the blight of cryptojacking. Instead of clearly announcing its presence and making specific demands, cryptojacking malware simply lurks in the background and saps the local processing resources to mine coins for the malware creator.

While the future of cryptocurrency remains as unclear as ever (and GPU prices have come down somewhat), there's still no shortage of people eager to mine for coins. There is also a glut of people who are unlikely to question a mild slowdown in the performance of their computers, which plays right into the pernicious hands of such malware creators. Consequently, I don't see cryptojacking drying up as the year goes on — meaning people should try to be more aware of unusual performance changes.

Biometrics will become more commonplace

Do you have a smartphone with a fingerprint sensor? If you've upgraded in the last couple of years, there's an excellent chance that you do, and the technology is moving quickly. We're already seeing in-display sensors (the OnePlus 6T being one of the earliest examples), and by now facial recognition has become commonplace through systems such as Windows Hello.

With security being an increasing concern, and "smart" devices attracting a lot of consumer interest, expect to see a moderate rise in the use of biometrics devices this year, being folded into multi-factor authentication to make progress on the path to secure digital wallets.

Cybersecurity spending will increase again

Average cybersecurity budgets increased significantly in 2018, according to the 2018 U.S. State of Cybercrime survey, which isn't a big surprise. The numerous high-profile data hacks spooked many businesses, and as more elements of their operations move online, businesses continued to increase their cybersecurity budgets.

Well, there's a strong chance that this trend will continue throughout 2019. The IoT is on the horizon (more on that next), and as the awareness of how catastrophically a hack can damage a business — particularly in the era of social media destroying company reputations — upping the cybersecurity budget to meet the growing threat is a sensible move.

IoT-suitable devices will provide fresh vulnerability

As much as consumers clearly love making their homes "smarter", they need to be aware of the risks involved with every new device that is given access to a system. In time, it will become very common for someone to have 30+ smart devices inside their home, and it will only take one of those devices presenting a security vulnerability to threaten the entire system.

Though we're not quite at that point yet, I anticipate alarm bells being sounded more loudly this year as the security-conscious try to warn us against the dangers. Unfortunately, these concerns will likely go unheeded, and people will mostly rely on manufacturers to do their due diligence. Will it all go wrong? Only time will tell.

Businesses will struggle to parse the impact of GDPR

When GDPR went into effect in 2018, plenty of companies weren't sure what to make of it. A lot of the impact it has had thus far has been somewhat...speculative, especially on the part of US-based companies that are unsure about the extent of their culpability. Despite the efforts of many to clearly explain what it all means, there remains a lot of uncertainty.
One of the biggest reasons for this is that the wider implications of the decision to implement GDPR may prove more significant than the regulation itself. They hint at a consumer-wide shift towards skepticism and a general lack of trust that businesses are going to treat their data with care, and this pressure is the primary source of panic for businesses.

There may come a time when companies feel confident enough to declare that everything they do is above board and within the letter (and spirit) of the law, but I don't think it'll happen quite yet. Perhaps 2020? In the meantime, they'll aim to work with companies that have great security track records (such as Shopify or Magento in enterprise ecommerce, or Barclays in the banking sector) to benefit from the association.

Identity fraud will get more sophisticated

The more information you share online, the easier it is for cybercriminals to piece the fragments of your identity together and assemble enough of a profile to impersonate you. And once they can impersonate you online, they can do anything from taking your money to using your name as part of a greater fraud. Older security standards typically had classic safeguards (sending mail or requiring direct visits), but much of multi-factor authentication is purely digital, exposing it to attack.

Factor in the development and distribution of tools such as FakeApp, the face-swapping tool that got a lot of attention last year, and you have many new viable avenues for fraud. Cybersecurity firms will need to stay ahead of the curve to combat this threat, and people will need to be cognizant of what's possible with today's technology — or else they may fall victim to it.

Will we see each one of these trends by the time the year is through? Not necessarily, but it wouldn't surprise me. They're all fairly safe picks. The central theme is one of rising complexity and the risks that come with it, and until the teething problems of developing technologies such as the IoT have been safely navigated, we must all be cautious.