



FOUR ONGOING CYBERSECURITY TRENDS THREATENING YOUR BUSINESS

By Janine Griffiths | January, 11th 2022 | IT Insights

 Facebook 0

 Twitter 0

 LinkedIn 0



Tech innovations are hailed for their potential to boost efficiency, increase profits, and generally make life easier for a business leader. While these promises are often delivered, innovation also brings with it new and increasingly dangerous forms of cyberattack. Hackers are in a constant race to tailor their efforts to the latest software and then change strategies before businesses can properly safeguard themselves. In order to successfully operate within such an unstable environment, it's necessary to understand the ongoing cybersecurity trends threatening your business.

ATTACKS ARE GROWING IN SOPHISTICATION

A quick look at any news outlet confirms that not only are cyberattacks becoming more frequent, but they are more powerful than ever. Ransomware has taken center stage, with this spring's WannaCry attack [infecting 300,000 machines in 150 countries](#). As the dust was still settling over this largest ransomware attack ever, [a new and even more powerful attack dubbed NotPetya](#) shook the world. These attacks crippled businesses, hospitals, schools, ATMs, and even caused chaos at nuclear power plants.

The progression of ransomware has been alarming. This dangerous software is being sold as a service, allowing those with no technical knowledge to purchase and deploy it with ill intent. It can even work offline, and some forms require no user interaction at all to infect machines. The latest attack appears to be the work of a professional hacker group, devoid of the bugs and killswitch discovered in WannaCry. Concerning for any field, the healthcare industry has even set up a Cybersecurity Task Force who just published a near [100-page report detailing cybersecurity as a public health concern](#), underscoring the seriousness of the topic.

HACKERS ARE FINDING NEW POINTS OF ENTRY

Internet of Things and cloud advancements practically define modern life, with so many objects seamlessly connected. However, many of these portals provide a vulnerable point of entry for an attack. Even a seemingly-innocent item like a teddy bear was recently used by an 11-year-old to demonstrate how the toy's Bluetooth connectivity could [hack into consumers' private cell phones](#) and access private information. Not only can IoT items be used to infiltrate a system to steal data, but [they can become weaponized](#) and used as a tool to attack other websites. Just as shocking, the massive security breach at Target in recent years was perpetuated through its [internet-enabled heating and cooling system](#).

Securing IoT devices and upgrading cloud security can help, but for every hole that is plugged many more appear. Your employees' mobile phones are vulnerable to cyberattack, and it's not just their personal information that is up for grabs. [Half of phones are at risk of exposing corporate data](#), as an organization typically has lesser control over an employee's cell phone. Hackers can take advantage of security lapses by using a personal phone as an entryway into a workplace system.

COSTS ARE INCREASING

As cyberattacks grow in ability and frequency, the costs incurred in combatting them grow as well. Ransomware cost organizations roughly [\\$1 billion last year](#), but paying money to get your files back is not the only factor impacting your bottom line. Businesses who fall victim to an attack can lose a significant amount of client and consumer trust. People expect their personal information to be protected, and a data breach can destroy confidence and hurt a company's image, subsequently hurting their sales or client relationships.

Additionally, it takes money to defend against cyberattacks. The WannaCry attack was carried out on machines that were running outdated programs. Organizations often neglect to update their computers due to cost, even when patches are made available to protect against specific new cyberthreats. [Overhauling network security](#) will likely require the hiring of specialized talent versed in the latest threats and solutions. It's no wonder that roles like [Information Security Analyst](#) are one of the highest-paying jobs in IT; it takes knowledge to implement security measures, and securing that talent takes money.

CYBERSECURITY TALENT IS SCARCE

Unfortunately, deciding to hire a cybersecurity expert is not solely a matter of money. As cybersecurity trends and methods of attack evolve, so too has the tech workforce. New security skill sets have been honed that can secure any business from the latest form of attack, but these individuals are a niche within an already small pool of tech talent. In fact, within three years there are expected to be [1.5 million unfilled cybersecurity roles](#) across the world. While there are a number of [recruiting strategies](#) and potential [solutions to the skills gap](#), it will still be difficult to locate and hire cybersecurity talent. With so many businesses and public organizations in need of these skill sets, competition is heavy.

CYBERSECURITY TRENDS THREATENING YOUR BUSINESS

Looked at as a whole, cybersecurity trends, threats, and solutions can be overwhelming for even the most tech-savvy business leader to consider. Innovations cause rapid change, leaving an unstable (and often unsafe) environment in which to operate. Your ability to locate and capture the best cybersecurity talent who can observe trends and alleviate threats will play a strong role in determining the overall success of your organization.

Looking for the best tech talent that can keep your business secure? [Contact us today.](#)

[« How to Recruit in a Fast-Growing Tech Hub
4 Ways Your Digital Presence Attracts Hard-to-Find IT Candidates »](#)




- [OUR STORY](#)
- [SEARCH TECH JOBS](#)
- [STAFFING REQUEST FORM](#)
- [BLOG](#)
- [CONTACT US](#)

CONTACT:

PORTLAND: 503.246.3989
DENVER: 303.953.4374
SALT LAKE CITY: 801.937.9646



CLEARLYRATED STAR RATINGS:

EdgeLink, LLC	
CLIENT RATING	TALENT RATING
 4.6	 4.8
BASED ON 43 VERIFIED CLIENT RATINGS	BASED ON 118 VERIFIED TALENT RATINGS
SEE ALL OUR RATINGS AND TESTIMONIALS	
	

[BACK TO TOP](#)