KRATIKAL
SECURE FOR SURE

2019

CYBER SECURITY PREDICTIONS

Cyber security is the most chaotic domain in the field of technology. Threats in this domain are ever increasing; various technologies are evolving rapidly, and sophistication in cyber attacks are increasing. This makes it difficult to access every pattern. Still, we have tried to list out few possibilities that we can foresee for the next 12 months.

01 RANSOMWARE IS NO MORE A TOP PAYLOAD CHOICE OF HACKERS, BUT STILL WRECKS HAVOC.

Ransomware is on the decline as hackers have shifted their interest to other attack vectors. Ransomwares attacks though have decreased voluminously, but have increased in sophistication. The reason for the decline is that invaders are finding other vectors more effective money-makers.

Ransomware isn't vanishing away anytime soon. Emails containing URLs is the most preferred way to infect computers. The best defense strategy against ransomware for any industry is to aware your employees about it, how it works, and what to do once you get infected from it.

02 DATA PROTECTION POLICIES WILL BE DRIVEN BY REGULATIONS AND PUBLIC SENTIMENTS ON PRIVACY.

The year 2018 observed some major data breaches in the history of cyber attacks, that too from top notch companies. Keeping the note of negligence of companies towards data protection, enforcement of GDPR and other privacy regulations are expected to be harsh.
Consumers are baffled by constant data leak occurred in the past few months. They are demanding that more default privacy policies should be applied for the protection of their data.
Companies rarely pay attention towards protecting their customer's data. The lack of privacy policies towards data or any sort of information may lead to EU implementing strict data privacy and other compliance regulations in the year 2019.

Facebook first shared data of around 50 million people with Cambridge Analytica, and later exposed data of around 87 million

03 SPONSORED TARGETED CYBER ATTACKS ON NATIONS AND SURVEILLANCE ON INDIVIDUALS WILL GROW.

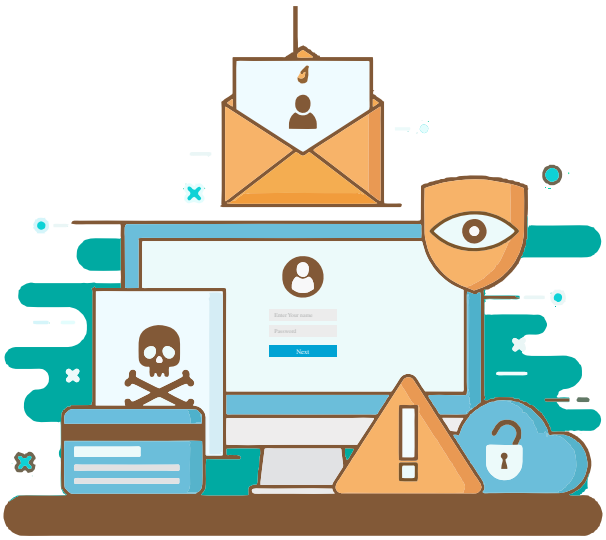
Sponsored targeted cyber attacks on nations and individuals will grow exponentially. Alike minded governments will sweep aside such attacks on their own land.
A recent case of such attack was reported when Saudi government used Israeli cyber weapons for tracking their own journalist Jamal Khashoggi while he was in Canada. Another famous targeted cyber attack on a nation was that of 'Stuxnet', when SCADA systems of Iran Nuclear Program were targeted from American and Israeli jointly built cyber weapons.
With advancement in cyber technology, attacks like these will only grow in the upcoming years.

04 MULTI-FACTOR AUTHENTICATION WILL BECOME THE STANDARD FOR ALL ONLINE TRANSACTIONS.

Most of the applications and websites will move on from password-only access. They will adopt various forms of multi-factor authentication. This won't be a perfect solution, yet it can be of a little help until a more standardized process is established.
Implementation of different types of multi-factor authentication techniques by companies will be slightly confusing for customers at start. With the implementation of these strategies, a standardized approach is expected to be generated and implemented.

05 NATIONS WILL MAKE AN EFFORT TO ESTABLISH CYBER WARFARE RULES.

Rules for any type of war sets certain boundaries that could help align much of the world against nations that cross them.
Various basic set of rules have been assigned for physical form of warfare, such as no slaughtering of civilians, no torture, no poisonous gases. As of now, no such rules exist for cyber warfare. This allows many nations to believe that they can do almost anything and can escape unharmed.



06 CYBER SECURITY TRAINING WILL CONTINUE TO MATURE. ORGANIZATIONS MIGHT REQUIRE MASTERS' DEGREE FOR

With the growing awareness of cyber security, training in this field will continue to mature. This means certifications alone will not be enough to acquire subsequent step for a security professional's career. Companies will emphasize more on Masters degree in cyber security for the positions of CSOs/CISOs.
The demand for the (cyber security) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million."

Information security analyst jobs are expected to grow 18% from 2014 to 2024 "

07 EMAILS AND COMPROMISED PRIVILEGES TO BE THE MAJOR CAUSE OF DATA BREACHES.

A company's security controls will continue to be bypassed by emails and compromised privileges. To reduce the risk of cyber attacks, organizations top priority should be to reduce the risk and impact of emails and privileges.

08 SPEAR PHISHING GETS MORE TARGETED.

Attackers are very well aware of the fact that the more data they own about you, the finer they can craft a phishing campaign against you. Tactics used by attackers in such campaigns can be a bit creepy.
One such example of a spear phishing campaign is when the attacker breaks into the email system, skulks and collects information about the victim. This gained information is then used to take advantage of the relations and trust built between victim and other people with whom the victim communicates on a daily basis.
A spear phishing attack can be highly effective, because the perpetrator can use tailored language to each individual.

65%
Phishing attempts have grown in the last year.

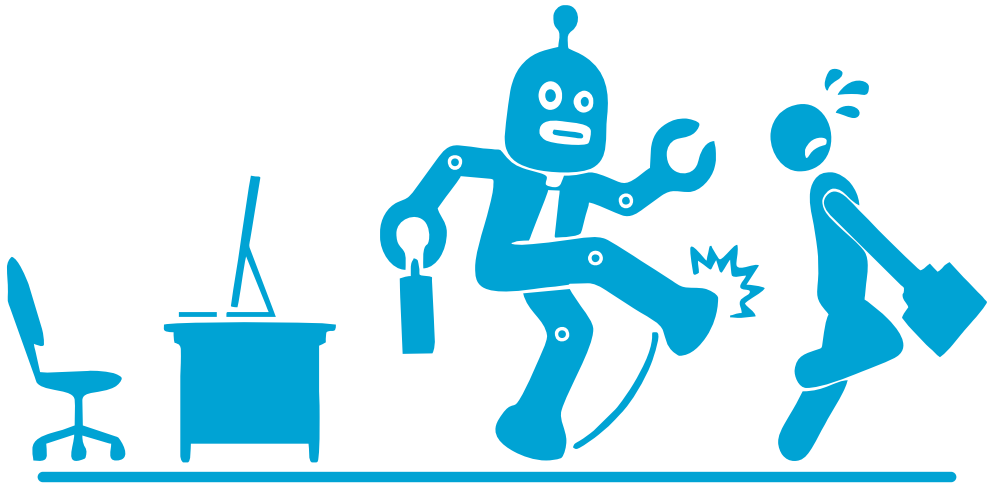
30%
Phishing messages get opened by targeted users.

12%
Those users click on the malicious attachment or link.

95%
All attacks on enterprise networks are the result of successful spear phishing .

09 MACHINES WILL ATTACK HUMANS.

With the increase in number of interconnected devices, there's a very high probability of machines attacking humans. Machines are much more effective at getting humans to click on malicious links. Most of such machines will be under the control of other human beings. AI models are built with a type of machine learning called deep neural networks (DNNs), which are similar to neurons in the human brain. DNNs make the machine capable of mimicking human behaviors like decision-making, reasoning and problem-solving.
With the help of IoT and AI, these machines have become the future assassins possibly causing physical harm to humans, eventually leading to death. This might lead to as far as your kids being chased by vacuum cleaners, your fridge getting automatically locked without your knowledge, or your car swerving into another car.
In short, every result of malicious act to attack humans in the cyber world will be easily executed with the help of these machines.



CONCLUSION

Cyber security companies like Kratikal provide end-to-end cyber security solutions. Our thrust on securing the People-Process-Technology has enabled us to offer impenetrable security to our clients across the world. Kratikal provides a complete suite of manual and automated managed security services . Kratikal also offers services like security compliance management. The company's flagship product, ThreatCop is a security attack simulator and awareness tool to automate the testing process providing real-time analysis of threats and vulnerabilities.