Recent cyber security computer network devices

1. Ready for the General Data Protection Regulation (GDPR)?

If your preparations for the European Union's new GDPR, explaining how companies should process, store, and secure the personal data of EU citizens are not complete, or at least well underway, then you better get moving. The GDPR will be enforced from May 25, and infringements can provoke fines of up to 20 million euros ($23.6 million at the time of writing) or 4% of the total worldwide annual turnover of the preceding financial year.

There's speculation about what will happen when the regulation comes into force, but the question of precisely how much non-compliance with the GDPR will cost will be answered soon. There's every chance the first few transgressions will result in punitive examples. We expect many organizations to be scrambling to adapt before May.

2. AI and machine learning can boost cyber defenses

As artificial intelligence and machine learning gathers pace, and starts to impact more and more industries, it's sure to play a bigger role in cyber security. Because the battle with cyber criminals moves so quickly, machine learning models that can predict and accurately identify attacks swiftly could be a real boon for InfoSec professionals. In the year ahead, these models need to be trained and honed. However, there is also a risk that AI and machine learning may be exploited by attackers.

3. Be proactive about ransomware

Ransomware has been a growing threat for the last few years, but it continues to claim high profile victims. It's not yet clear what everyone learned from the WannaCry ransomware attacks, but we hope that it highlighted the need to back up regularly, keep patching and updating systems, and strengthen your real-time defenses. If organizations took these simple steps, we could dramatically reduce the impact of ransomware.

4. Handling data breaches gracefully

It may prove impossible to eradicate data breaches completely, but every organization has the power to lessen the blow by handling the aftermath correctly. Equifax gave us a masterclass in how not to handle a data breach earlier this year. By delaying disclosure, misdirecting potential victims, and failing to patch a known vulnerability, it made a bad situation much worse. We can only hope this proves instructive for others in the year ahead.

5. The IoT is a weak link

We're rolling out more and more sensor-packed, internet-connected devices, but the Internet of Things remains a major weak point for defenses. All too often these devices lack basic security features, or they aren't properly configured and rely upon default passwords that can give attackers easy access. This in turn is giving rise to botnets, which can be used for volumetric attacks, to exfiltrate stolen data, to identify further vulnerabilities, or for brute force attacks. We need to properly secure the IoT or it will continue to be a big issue in 2018.

6. There's still a skills shortage

The dearth of skilled cybersecurity professionals continues to be a major problem for many organizations. Even with average InfoSec salaries soaring, there are thousands of vacant positions. This is leading many companies to engage external cybersecurity services and virtual CISOs. We expect to see more outsourcing as employers try to find a way to fill the skills gap.

7. Developing a common language

While the specter of multiple threats looms, there are also positive developments in the cybersecurity realm, not least the creation and adoption of things like NIST's Cybersecurity Framework. As more organizations and cybersecurity experts come together to develop a common language, our collective defenses grow stronger.

8. Patching and application testing

It's not shiny or new or exciting, but it should still be top of mind. The number of data breaches in 2017 that were made possible by known vulnerabilities and a sluggish approach to patching is horrifying. It's not enough to identify problems – you must act. Application testing falls into the same bucket, in that it's too often ignored. If you don't test your security, then you don't know how secure your application is. If everyone put a fresh effort into patching and app testing in the coming year, we would see a dramatic drop in data breaches.