LogRhythm Labs

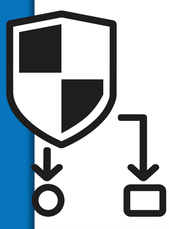
10 Security Intelligence Predictions for 2016

1 An uptick in all-in-one home surveillance systems

We are seeing more motion sensing/camera/recording devices in the home that can be managed through personal devices. This type of technology will continue to expand, and with this expansion, hackers will try to exploit them or cause chaos.

2 A rise in the use of mobile wallet apps

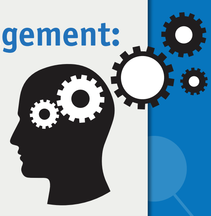
Like having virtual money and an ID in one's pocket, mobile wallet apps are at the intersection of marketing and payments. And although a mobile wallet is convenient, it is directly tied to one's mobile phone which is a critical access vector for cyber threats.



3 A new model of what to protect

Instead of a mandate to "protect everything on the network," IT staffs must work more like a unit, centralizing and protecting the most critical resources. This approach moves defense-in-depth to the most critical business components of the organization.

4 Identity access management: The unsung hero



Companies will be investing more money and R&D resources in behavior-based modeling, analytics and identity access management to track behaviors. More customers are asking about it, which will motivate the rest of the industry to follow.

5 The next big attack target: Education

This industry has a plethora of data that cyber criminals want—credit reports, personally identifiable information (PII), donor money and tuition. And these institutions are not doing an adequate job of securing all their systems. Add to that the myriad "customer"—professors, student, parents, administrators—and you have magnified the attack vectors exponentially.

6 Emergence of hacking for good

More organizations, like Anonymous, will be leaving the dark side and hacking for the public good. They are more motivated by the notoriety and publicity on social media than for financial gain. Teens are learning to program on their own; high schools are introducing technology and coding to get this generation aware of and more proficient in this industry. Younger generations are finding coding and programming cool. This is the next-gen workforce that we hope will continue to want to positively impact society.

7 Security is in a renaissance

Security is a hot space. And the fact that CISOs are getting a seat in the boardroom is another indication of the importance of this industry for all organizations, regardless of the vertical market. Many companies still don't have adequate security infrastructures, awareness or training to defend themselves. There will also be consolidation. Companies will either "get it" or not, and governments will start ramping up regulations.

8 Next steps for CISA, open sharing of threat intelligence

Critical infrastructure will emerge as more companies in various sectors, such as energy, financial and healthcare, join in. The principle and the intention behind the creation of a more collaborative community for the open sharing of threat intelligence is grand, with two distinct sides of the political aisle. We will either see a big push or nothing happen at all.

9 Ransomware will gain ground

The ransomware-style of attack is powerful and expanding into Macs and mobile devices, making it easier to target consumers. Criminals can gain big profit by locking down an entire system; victims have no choice but to pay. Although consumers are ripe for the picking, businesses are not immune to this approach.

10 Vendors will need to step up

Despite the running list of breaches, many companies still do not have an adequate security infrastructure to defend itself against cyber criminals. We cannot rely on consumers to know how to protect home systems. It is up to the security vendors to build better software, systems and patching mechanisms, as well as offer training and services to protect people, companies and their assets.