5 Cybersecurity Trends
To Watch For In 2016

1. The Unintended Consequences of Government Intervention

Conflicting official involvement in cyberspace in 2016 will create the threat of collateral damage and have unforeseen implications and consequences for all businesses and organizations in the US.

Even organizations not implicated in wrongdoing will suffer collateral damage as authorities police their corner of the Internet.

Legislators will always be paying catch up, they will always be talking about yesterday, while cyber-threat is always talking about tomorrow.

TRIDENT CAPITAL CYBERSECURITY

2. Big Data Brings Big Problems

Organizations are increasingly embedding and relying upon big data in their operations and decision-making process. But it's essential to recognize that there is a human element to data analytics and those who fail to respect that human element will put themselves at risk by overvaluing big data output. The investment says you must believe the outcomes.

One of the hidden security risks is not necessarily people stealing that information but actually manipulating it in ways that the owners will never see.

Provenance is all important. As soon as organizations starts sharing their big data, they open themselves to substantial risks. Knowing how the information is being used, who it's being shared with, who's adding to it and how it's being manipulated is key to managing that risk.

3. Mobility and IoT

At the risk of beating a dead horse, smartphones and other mobile devices are creating a prime target for malicious actors in the Internet of Things (IoT).

There are an increasing number of workers that are constantly mobile and the demand for that mobility is forcing developers to work under intense pressure and on razor-thin profit margins which is sacrificing security and thorough testing in favor of speed of delivery and low cost.

The result is poor quality products that are more easily hijacked by criminals or hacktivists.

CIOs should be proactive in preparing the organization for the inevitable by ensuring that apps developed in-house follow the testing steps in a recognized systems development life-cycle approach.

They should also be managing user devices in line with existing asset management policies and processes, incorporating user devices into existing standards for access management and promoting education and awareness of BYOD risk in ways that reach their audience.

4. A Perfect Threat Storm

Cybercrime, along with the surge in cost of compliance to deal with the uptick in regulatory requirements and the relentless advances in technology against a

backdrop of under-investment in security departments, have all combined to cause the perfect threat storm.

There is an increasing maturity and development of the cybercrime gangs and they have become incredibly sophisticated and well-coordinated. We're seeing an increase in crime as a service. You can no longer predict how a cyber-criminal is going to come after you.

We have viewed cybercrime from the perspective of it being an external attack, so we have attempted to throw a security blanket over the perimeter. But there is now a threat within which creates a very uncomfortable place from an organizational standpoint.

Many companies believe that with big data analytics, they have complete visibility across the entire organization. The cybercriminals have had that capability for ages. Our approach is continually reactive as opposed to proactive. Until that changes, we are in for a long uphill battle with lots of casualties.

5. The Skills Gap Could Become A Death Knell

The information security profession is maturing just as the increasing sophistication of cyber-attack capabilities demand more increasingly scarce information security professionals.

While cybercriminals and hacktivists are increasing in numbers and deepening their skill-sets, the "good guys" are struggling to keep pace.

The problem is going to grow worse in 2016 and beyond as hyper connectivity increases, and CIOs will have to become more aggressive about getting the skill sets the organization needs.

In 2017, we're going to become very much more aware that we don't have the right people in our security departments. We've got some good technical guys who can fix firewalls and that sort of thing, but the absence of cybersecurity being linked to business challenges and business developments is a significant weakness.

Boards must come to the realization that cyber is the way they do business. We still don't have the joined up linkage between the business and the security practice. Until we do, we are ill-equipped to do battle with cyber-criminals, and we will continue to lose.