cioxchange
Driven by CIOs, fueled by Gartner

DACH
30 November 2017
Frankfurt, Germany

Driving Business Transformation: Leadership in a Digital World

5 Trends in Cybersecurity for 2017 and 2018

Gartner's top cybersecurity trends cover the skills shortage, cloud and a shift to detection and response.

In the every changing world of cybersecurity, there are a few truths about what leaders want. Cybersecurity leaders seek:

- Balance risk, resilience, usability and price
- Require enough visibility into what is happening
- Gain more control–but only over what matters

But there are hard realities that govern cybersecurity.

"You can't protect everything equally…we have to find a way to control only what matters," said Earl Perkins, research vice president, during the Gartner Security & Risk Management Summit 2017 in National Harbor, Md.. In fact, security experts should know four things: you can't fix everything, you can't make assets fully secure, you can't know how secure they all are, and you can't know how secure your digital partners are.

However, in a world of unknowns, five cybersecurity trends appear for 2017/2018.

Skills and organization for cybersecurity continue to change

With a zero percent unemployment rate, security skill sets are scarce. The industry needs and will continue to need new kinds of skills as cybersecurity evolves in areas such as data classes and data governance. It's a problem that security experts have avoided, but the reality is that in the next three to five years, enterprises will generate more data than they ever have before, said Mr. Perkins.

Changes in cybersecurity will require new types of skills in data science and analytics. The general increase in information will mean artificial security intelligence is necessary. Adaptive skills will be key for the next phase of cybersecurity.

Cloud security becomes a top priority for many

As the cloud environment reaches maturity, it's becoming a security target and it will start having security problems. It's possible cloud will fall victim to a tragedy of the commons wherein a shared cloud service becomes unstable and unsecure based on increased demands by companies. When it comes to cloud, security experts will need to decide who they can trust and who they can't. Companies should develop security guidelines for private and public cloud use and utilize a cloud decision model to apply rigor to cloud risks.

> *continued on next page*

cioxchange
Driven by CIOs, fueled by Gartner

> *continued from previous page*

Shift your focus from protection and prevention

"Take the money you're spending on prevention and begin to drive it more equitably to detection and response," said Mr. Perkins. "The truth is that you won't be able to stop every threat and you need to get over it."

A dedicated, well-financed actor who is after something in your enterprise is going to get it, even if they use the weakest link–people–to do so. This means adapting your security setup to focus on detection, response, and remediation. That's where the cybersecurity fight is today. In the future it will most likely move to prediction of what's coming before anything happens.

Application and data security are led by development operations center

There is a new window of opportunity in application security, but most enterprises don't take advantage of it because of the expense. It's time to figure out the right way to evaluate the value of security and the best way to explain that to the business.

Additionally, DevOps should become DevSecOps, with a focus on security. This is a good time to marry development and operations. The time to market has shortened so much, it creates an endless connection between development and operation, which means it's important to stop running them as isolated units. This is the time to bring security to DevOps, or if the team is not internal, to ask the service provider what kind of security they provide.

Digital ecosystems drive next generation security

Safety, reliability and privacy are also a part of cybersecurity. When these systems begin to have a direct physical impact, you now become responsible for the safety of people and environments. Without a handle on security, people will die. The reliability portion is essential for operation and production environments or anyone in asset-centric firms.

Gartner analyst Earl Perkins, research vice president, presents five cybersecurity trends during the Gartner Security & Risk Management Summit 2017.