## How Will Companies Meet Cyber Security Threats in 2018?

With ransomware attacks costing three companies between $200 and $300 million each in 2017, organizations are being forced to review their current security vulnerabilities and recognize the threat of cyber-attacks as a core business risk.

Improved security will come at a cost. A Gartner survey released in August 2017 predicts a seven percent increase in cybersecurity spending by year's end, to $86.4 billion. This is expected to increase to $93 billion in 2018, with key areas of investment including data loss prevention, advanced threat protection, and application security testing.

Security services and solutions will certainly proliferate and grow in complexity, but as Tenable's Chairman and CEO, Amit Yoran points out, the WannaCry and Petya attacks of 2017 were based on threat methodology that had been around for some time.

> "This is not some super-elite hacker. Not some nation state, a sophisticated thing coming down. It's the basic blocking and tackling that people just still don't get, they still aren't getting basic hygiene.´"

Chris Jordan, CEO of Fluency, makes a similar observation:

> "The biggest issue in security is keeping customers focused on the basics. People tend to want what's new in the security world. Good infrastructure is boring, but most organizations need that. … Most CIO/CISO's focused on recovery systems as a long term solution. While new EPP/EDR solutions seem sexy, the boring backup and recovery has saved the day."

Another problem cited repeatedly is the tendency to employ a large number of security solutions. Trend Micro notes:

> "Too many security solutions can easily translate to numerous protection issues, especially in regard to visibility, training, manageability, and updating. If employee users aren't trained properly, they will not leverage solutions in the most valuable way for the corporation."

Looking ahead to 2018, companies are advised to:

- Consolidate services and solutions--after a careful audit to assess the capabilities of security solutions currently in place

- Choose one or more security firms to partner with to come up with best overall protection scheme

- Find intelligent solutions to help manage their cyber tools, given the difficulty of hiring sufficient security personnel

Organizations can also turn to a number of next generation threat prevention tools that don’t require as much daily monitoring from staff as older solutions do.

*[End here or include something on the company.]*

n