N.J. businesses should brace for higher cyber security costs, complexity, experts warn

By Ed Beeson/The Star-Ledger
on January 15, 2013 at 8:13 PM, updated January 15, 2013 at 8:45 PM

Cyber security will become an increasingly complex and costly part of doing business, but caution and preparedness is a better alternative than getting hacked or duped by cyber thieves, security experts said today at a conference on the problem.

Information technology managers are grappling with new vulnerabilities and security risks as companies move more of their networking operations off-site and into the so-called data cloud, and as more personal computing is done on smart phones and mobile devices. Companies are also facing increasingly high stakes for preventing security breaches, as both clients and the government demand that they do more to protect themselves from security lapses.

"In the trenches, every day you just feel overwhelmed," said Gideon Lenkey, a consultant who runs Ra Security Systems, which advises companies on cyber security. "We're small teams going up against very refined, almost military operations."

Outbreaks of attacks in recent months and years show a growing push by organized crime, sovereign nations and Internet activists to exploit weaknesses in the data security of U.S. networks and their users.

The websites of large banks, for example, have been hit with what are called denial-of-service attacks. Last week, PNC Bank told customers in an email that it appeared to be the latest victim. While banks have not reported sensitive customer data being stolen during these attacks, their websites have repeatedly crashed, forcing customers to bank offline.

This week, the hacker collective known as Anonymous claimed credit for a denial-of-service attack on the Massachusetts Institute of Technology's website. The group initiated the attack following the apparent suicide last week of Aaron Swartz, a pioneering programmer who faced federal charges that he hacked into an M.I.T. website and accessed millions of academic papers held in a subscription service.

While companies worry about external attacks on their networks, many times the biggest threats come from within, security consultants said yesterday at the conference, held at Raritan Valley Community College in Branchburg. Often, it is the careless worker who falls prey to an Internet scam while using a device connected to their company's network, they said.

A big concern for IT managers is the growing demand that companies let their workers use their own personal devices – be it laptops, tablets or smart phones – to connect with a company's servers. Known as Bring Your Own Device, or BYOD, the trend is proving to be "a nightmare for IT managers," said Jerry Ravi, a senior manager for EisnerAmper's consulting services.

"Now they have to secure something they don't have control over," he said.

Small businesses, which typically lack the IT expertise, are particularly vulnerable and appear to be more of the focus of hackers' attention, panelists also noted.

A 2012 Verizon survey of business data breaches found that restaurants accounted for most of the incidents. More than half, or 54 percent, of the 855 security breaches surveyed by the telecommunications giant took place at food services and accommodation businesses, with the overwhelming majority of these at restaurants. Another 20 percent of breaches hit retail businesses, the report found. Most of these involved the theft of patrons' credit information.

But the attacks on financial institutions, while lower in occurrence, saw greater numbers of customer records being accessed and stolen. The more records that get stolen, the more expensive it is to clean up. A Congressional Research Service study issued last fall found that a breach cost companies on average $214 per record stolen, or about $7 million per incident, according to data cited by the Arianna Frankl, an attorney with Cole Schotz Meisel Forman & Leonard.

A sign of the growing threat is the emergence insurance policies to help businesses deal with the costly aftermath of a cyber attack.

Because standard policies typically will not protect from a cyber attack, insurers are introducing specialty coverage that can help defray costs of a breach, according to Elissa Doroff, an advisory specialist with global insurance broker Marsh. This can include the costs of notifying customers, conducting forensic investigations and even liability from class action lawsuits, she said.