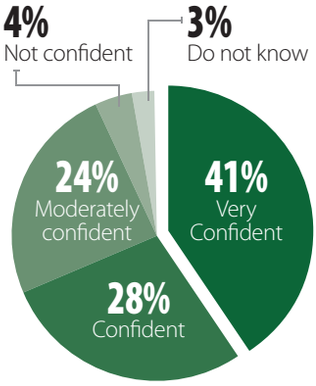
CYBER BOMBS: DATA-SECURITY SECTOR HOPES ADOPTION WON'T REQUIRE A 'PEARL HARBOR' MOMENT

BY RODNEY BROWN | MASS HIGH TECH STAFF

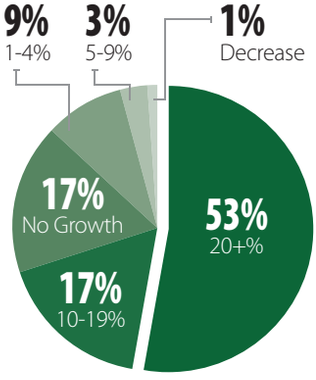
TECH PULSE

MHT surveyed more than 300 mobile companies during the third quarter 2011, asking them their plans for hiring, status of venture investment, confidence in the economy and more. Here's what they told us:

QUESTION: HOW CONFIDENT ARE YOU THAT THE REGION'S TECH SECTOR CAN MAINTAIN POSITIVE GROWTH OVER THE NEXT 12 MONTHS?



QUESTION: DOES YOUR COMPANY PLAN TO INCREASE THE SIZE OF ITS LOCAL WORKFORCE IN THE NEXT 12 MONTHS?



SOURCE: MHT RESEARCH

The data security sector in New England continues to grow, despite the almost Sisyphean task it faces — getting people to use it. Or, in the words of **Steven Sprague**, CEO of Wave Systems Inc.: "The auto industry can put a seatbelt in every car, but that doesn't mean people will wear them."

Driving that growth is a seemingly unending wave of cyberattacks on corporate data and private information, along with an explosive growth of connected users and devices.

Slow adoption of data security doesn't mean the industry isn't growing fast enough to allow Lee-based Wave Systems to attract investor interest and increase its top line. The 250-employee maker of data protection software and hardware-based tools recently raised $11.1 million in an offering of equity to its investors that was used to help fund its $12.8 million acquisition of Israeli security company Safend Ltd., which makes similar endpoint data protection tools as Wave Systems, such as port and device control and encryption for removable media.

Buying Safend gave Wave Systems a chance to expand its presence in Europe and the Far East, and that growth for the company — and the sector in general — is driven by a coincident pair of occurrences, Sprague said. "There's definitely a change under way, and that is being brought on by two things," he said. "One is the increasing number of attacks that we hear about every day and the other is the increasing use of mobile devices being used in the enterprise, with no real security in them to speak of."

Sprague said, however, so far no single hack has been big enough to be a wake-up call.

"I think for all of us in the industry the real concern is that we hope we don't have to have a significant event," he said. "The question is when do you have a 'Pearl Harbor' of cybersecurity — and will that get them focused on the problem?"

CYBER SECURITY CENTER LAUNCHES

Getting people and businesses to take data security seriously is one of the three pillars of the newly established Advanced Cyber Security Center, a collaboration bringing together government, industry and academia in Massachusetts to advance data security. While the ACSC, which has its headquarters at MITRE Corp. in Bedford, also has the mission of sharing data about threats and attacks, and promoting university research and tech transfer spinouts into new startups, its toughest objective may be around establishing public policy and legislation.

Gary Gagnon, corporate director of cyber security at MITRE, also hopes that there won't be a 'Pearl Harbor' cyberattack, and that the increasing number of attacks overall will get the attention the issue needs.

"It doesn't take one incident to bring this sort of community together," he said, at the

launch event for the ACSC in September. "It takes many more."

One Bay State company trying to help stem that tide is Aveksa Inc. of Waltham. Just last week, Aveksa announced a new product that it hopes will make it easier for companies to adopt secure data access, and solve one of the major roadblocks to widespread cybersecurity adoption: inconvenience.

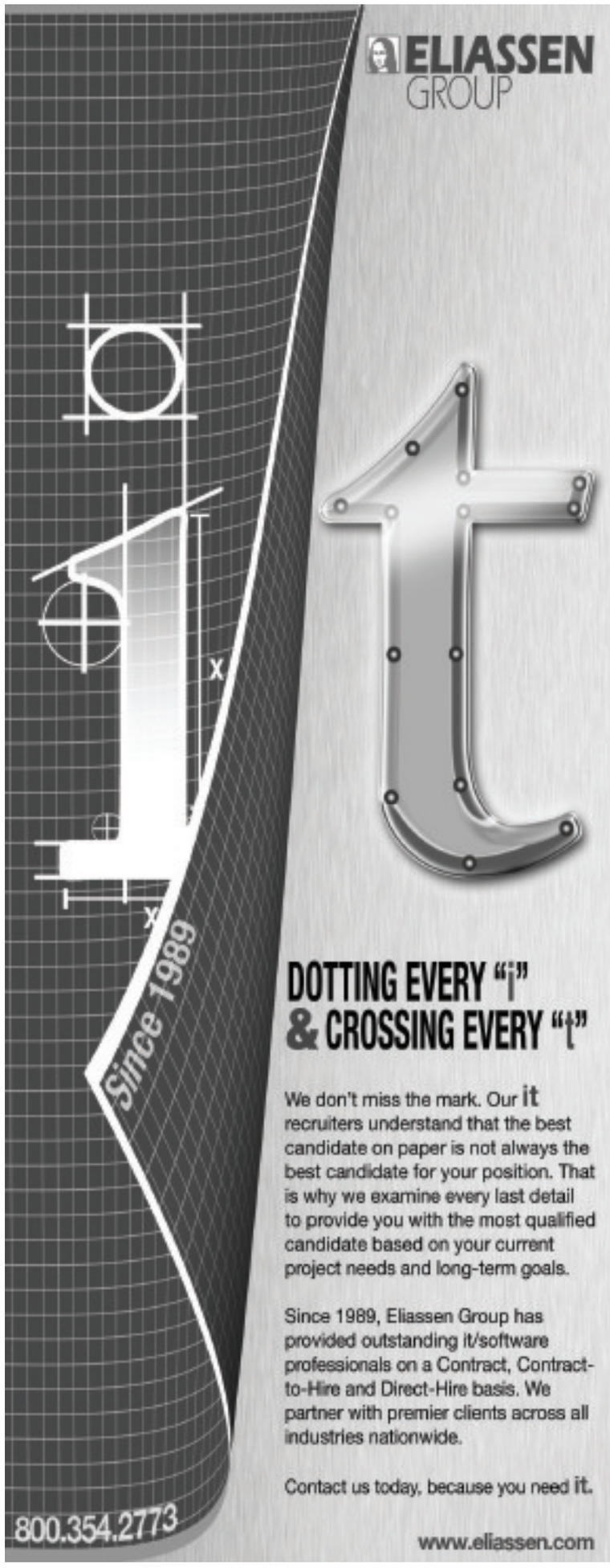
Aveksa's new product is called Access Fulfillment Express, according to **Jason Garbis**, vice president of marketing. AFX is built on an open-source service bus, allowing enterprise customers to modify it for their own needs at will. "These are all technically advanced organizations, and they have the resources to be able to customize this," Garbis said.

Garbis hopes that the new AFX product kicks the company's already solid growth into overdrive. Now at 85 employees, Aveksa has more than doubled its sales force since the beginning of the year, and Garbis said, "We have a pretty aggressive growth plan for hiring." He anticipates growth in the range of 25 percent to 30 percent over the next year, but that could explode if the use of data security takes off, as every expert says it must.

SEC ISSUES DATA-BREACH GUIDANCE

To help that along, the U.S. Securities and Exchange Commission has finally addressed the topic, issuing guidance for public companies on reporting data breaches. On Oct. 13, the SEC said in a memo from the Division of Corporation Finance that public companies should include cyberattacks in the statement of risks within financial filings with the SEC.

The new guidance, however, is just that, and is not an enforceable rule, the SEC division points out. Without a real stick from the SEC or federal legislation, what little carrot there is can be happily sacrificed by companies as part of the cost of doing business, said Wave Systems' Sprague. And that is unfortunate, because such breaches keep funneling money to the hacker and cyber criminals who can keep expanding and improving their attacks.

"Its almost like if you look back at Prohibition funding the mafia," Sprague said. "The challenge we have today is that we are in that kind of situation with cybercrime. It generates billions of dollars for criminals, but we don't care because it isn't affecting our accounts, and the banks don't care as they pass the cost along to the merchants."

Or, as MITRE CEO **Alfred Grasso** put it at the Advanced Cyber Security Center launch event: "The attacks are becoming increasingly more sophisticated; the current solutions are inadequate.