

Reuters
Microsoft
says to buy
LinkedIn for
\$26.2 billion

FOX Business
Why HBO
Now's
Success is
Good for
Netflix

US News &
World Report
Google wants
to tap the
second
golden age of
television

Associated
Press
Entrepreneurs
pitch products
to QVC

Associated
Press
Channels go
dark for
millions of
Dish
customers

We apologize for the brevity of today's NewsClips. Today's news is dominated by the terrorist attack in Orlando. Our thoughts and prayers are with the victims and their families.

A longtime Villanova professor accused of accessing child pornography on a campus computer in March had someone looking over his shoulder: a security firm that the university had hired to monitor its computer network.

Within 20 minutes, BTB Security identified the building and floor where the computer was located and alerted Villanova, kicking off an investigation that led to the arrest of Christopher Haas, a tenured associate professor of history and classical studies.

The discovery was one of many security breaches that BTB, a cybersecurity and digital-forensics company, says it uncovers for clients every year.

On the seventh floor of a nondescript redbrick building in Bala Cynwyd, employees monitor computer networks of more than 150 clients, 24/7, 365 days a year, said Ron Schlecht Jr., managing partner of BTB, which stands for Beyond the Basics.

They look for hackers, viruses, unusual access of foreign web addresses, removal of intellectual property, child pornography, and other violations of law or company policy.

Their employees also play offense. They try to break into clients' companies - both by computer and in person - to identify security weaknesses and help correct them. Wearing small body cams, they show up as copier repair employees, delivery workers, bug sprayers and auditors, talking their way into computer rooms, bank vaults, and other sensitive areas. Then they present a report to clients, with video.

"We do bad things to good people so bad people don't do the bad things to good people," Schlecht said.

Citing the pending case against Haas, BTB officials declined to discuss specifics of the Villanova matter beyond the description provided by the company spokesman in April after Haas' arrest. Villanova also declined comment on Haas' case but said that it has worked with BTB for two years as part of a larger information-technology security strategy.

"Safeguarding the security of the Villanova community - including protecting the university's information assets - is an important strategic initiative which we take seriously," spokesman Jonathan Gust said in a statement.

On a recent afternoon, BTB executives offered a glimpse into their security operations and discussed their decade-old business aimed at keeping their clients safe from both intruders and insiders who break company policies.

BTB sometimes is hired in response to a data breach and other times brought on to assess a company's security.

On the defense, BTB has found a plethora of violations, including one company with an

information-technology employee who had "an extremely large repository of pornographic materials on company servers," said Brian Bailey, also a managing partner at BTB.

"We found people hosting their private company businesses out of an employer's data center," Schlecht said, "and others pushing off . . . intellectual property to competitors to try to get a job."

The company's clients include financial firms, health-care companies, resorts, and colleges. He declined to identify clients.

BTB executives would not allow a reporter and photographer to enter its security operations center.

But, he said, "they're right behind us" and flipped a switch that turned the conference room's opaque glass clear, revealing five employees in front of computer monitors, studying data.

When an alert comes, employees explore it. If the threat looks real, the company notifies the client and works with it to investigate and remedy the problem, Bailey said.

The average client experiences about 10 security issues a month that BTB helps to combat, Bailey said. In some cases, BTB wards off what looks like a hacker trying to take control of a company's information to hold for ransom.

"As soon as we see that type of malware get introduced into the environment, our alerts start going nuts," Bailey said.

BTB recently discovered a Russian hacker who had slipped through a client's firewall, he said. Half the time, the hackers are foreign, Bailey said, and "typically, organized crime."

"We also looked at once they got in, what did they do," Bailey said.

Employees also investigate unusual access of foreign websites, looking at the user and the user's computer history.

BTB also tells clients when it sees violations of company policy, such as pornography views.

"There are things we may see that are indicators, a website address," Bailey said.

When employees spot suspicious activity, they can pinpoint its origin, down to the physical location and the computer.

"It may say 'seventh floor, port 42,' " Schlecht said.

After BTB's discovery at Villanova, Haas was charged with hundreds of counts of accessing pornographic images, stemming from a 2012 federal probe in which authorities allege they found more than 400 pornographic images on a Villanova-issued laptop at his home. He faces trial in October.

In-person visits to clients often make for the best watercooler conversation, Schlecht said. He recalled the time he tried to penetrate the loading dock computer system of an Atlanta retail company. An employee stopped him and left to call for help. He sneaked in and gained access. The employee caught him on his way out.

"He got physical with me and dragged me out the back," Schlecht said.

As the employee began to call 911, Schlecht showed him a letter, authorizing his visit.

"He was still angry."

David Williams, BTB's director of security operations, is recognized by his colleagues as one of the best infiltrators.

"I recently broke into a bank by pretending to be a copier repairman," Williams said. "I came in a polo shirt with a logo on it and acted like I was supposed to be there."

He also got into another bank's vault, wearing a suit and claiming to be an auditor, he said.

"It's definitely a lot of fun," he said. "I get to break into companies for a living and improve their security, as well." – *Philadelphia Inquirer*



127 State Street, Harrisburg, PA 17101
717.214.2000 • bcaps.com

First in Broadband.
The Future of Broadband.®
