Candidate for K-State's head IT job previously hit by cyber attacks

Jul 21, 2017 http://www.kstatecollegian.com/2017/07/21/candidate-for-k-states-head-it-job-previously-hit-by-cyber-attacks/

Will Laney, an interview finalist for the top information technology security job at Kansas State, was unable to stop three cybersecurity attacks in the span of about a year during his previous position at the University of Oregon.

Laney, who was chief information security officer at UO through June 2017, was interviewed July 17 for the director of identity, security and compliance at K-State.

The cybersecurity incidents during Laney's previous occupation were all related to hacked network printers on the UO campus. The printer log-ins were compromised by hackers and the campus's printers were forced to print fliers with racist, violent content on three separate occasions.

Laney reported after each of the 2016 incidents as "looking into changes with the way printers operate" and said "the university has taken proactive steps to minimize the hack."

However, university police spokesman Kelly McIver told the Daily Emerald, UO's student newspaper, the printers compromised in the most recent exploit lacked passwords and had their unsecured IP addresses were freely accessible to anyone through the internet. When recently contacted, McIver said the reported printers were secured by the institution's information services department.

"We knew some units had not secured their printers but assumed they would in time as we kept letting them know," Laney said. "We were also working with the network team to set up networks for printers which were internal only, so they could not be pinged from the internet.

A string of racism and anti-Semitism

Four printers at UO were put out of commission after they were hacked and printed ink-heavy images of the Shahada, the Muslim declaration of faith, for several minutes in July 2015.

All affected campus printers were blocked, Laney said, and the owners of printers found in network scans with default passwords were reached out to.

them. However, contracting issues delayed the implementation until December 2016. Until then, Laney said, his team was asked to stop scanning the network and fixing printers for what they assumed would be a brief pause.

The following spring, a coordinated cyber attack hit numerous colleges and universities, including more than 100 printers at UO that spread swastika-laden fliers that directed white men to a neo-Nazi website in March 2016.

Information technology services at UO again scanned the network for default passwords and blocked the impacted printers, Laney said. While many of the printers affected this time were recently purchased with default passwords still in place, others remained uncorrected from the earlier provocation. Vulnerable departments were notified biweekly, and CTX helped UO IT address ongoing security flaws.

Andrew Auernheimer, a member of a larger anti-Semitic network of computer hackers and a key player behind the March attack, again gained control of a number of unsecured printers at universities — UO among them — in August 2016.

This time, printers circulated leaflets calling for "extreme violence" against racial and ethnic minorities, encouraging "the killing of children" and praising a Norwegian terrorist convicted in a 2011 bomb attack that claimed the lives of 77 people. Auernheimer claimed in a blog post that he used a common tool to pinpoint and communicate with "upwards of a million devices" that were remotely accessible from his home in Ukraine.

"Our information services department has used these occasional unauthorized printing episodes as a way to educate and correct these unintentionally insecure situations," McIver said, noting that none of UO's data was compromised. "The only loss was the paper and toner that printed a very few copies of an offensive, reprehensible document that was seen by only a few people."

The state of cybersecurity at K-State

"This is the first I'm aware of it," Rob Caffey, interim chief information officer at K-State, said when interviewed about the UO printer incidents July 14. "It seems like it keeps happening over and over again to him, right?"

Caffey said the past colleagues and employers of both IT finalists would be followed up with after the two applicant interviews July 17.

K-State's IT staff has been reviewing incident response procedures based on the WannaCry ransomware attack last May, in which many hospitals, governments and corporations around the world were hit with a computer virus the National Security Agency has linked to the North Korean government regime.

The more distributed control of devices and electronic security at UO, in which departments may connect newly purchased and unsecured devices to the internet without informing the university's central IT services, created a vulnerability K-State would like to avoid, Caffey said.

The number of compromised K-State eIDs already exceeded the 2016 on total May 1, 2017, according to K-State Information Technology Services. Of the 1,521 people who unwittingly gave their passwords, 60 percent were students.

In the job listing, K-State Human Capital Services describes the director of identity, security and compliance position as "responsible for the planning, development and implementation of the university's overall information systems security program," in addition to "protecting and defending against unauthorized access to systems, networks and data."

As part of his application, Laney wrote that as the first chief information security officer at the University of Oregon, he developed "policies, procedures and guidelines, perform[ed] security incident response," and "lead the risk management effort."

"We're trying to enhance our security posture, and part of that effort is to fill this chief information security officer position that will hopefully lead that effort to try to make sure that we are secure against those kinds of attacks," Caffey said.