3Qs: How hacking will affect credit-card holders

April 5 2012, By Brenna Eagan

William Robertson (left), assistant professor in the College of Engineering and the College of Computer and Information Science, is seen here at a congressional briefing on cybersecurity last month in Washington that was led by a Northeastern University team of experts. Credit: Paul Morigi

Last Friday, a major Atlanta-based payment card processor, Global Payments, announced a server security breach that could affect more than 1 million accounts. We asked William Robertson, a cybersecurity expert and professor in both the College of Computer and Information Science and the College of Engineering, to explain how hackers penetrated the company and the impact this will have on credit-card holders.

How did the Global Payments security breach occur?

The breach was only made public on Friday, and the story is still developing. Nevertheless, it seems clear that cybercriminals have had illicit access to the internal networks of Global Payments since January 2012, and possibly as far back as January 2011. The company has stated that at most 1.5 million accounts have been breached, although this number may increase as the investigation proceeds and more details become public.

From what we do know, it appears that hackers successfully penetrated a subset of the servers that comprise Global Payments' card processing system. From this vantage point inside the company's internal networks, the hackers were able to exfiltrate sensitive credit-card data, including sufficient information to clone new, illegitimate credit cards. The intrusions themselves could have been a result of poor password selection, exploitable network services or even targeted attacks against highly privileged employees. At this point, however, there is no way to be sure what the exact vector was.

Can hacks like this be prevented? If so, what measures is the cybersecurity industry or even government putting in place?

While we do not yet know the specifics of this case, it is clear that our current computer systems and networks are fundamentally insecure in the sense that we have little assurance that they are free of security vulnerabilities. And, even if they were perfectly secure, cybercriminals could still attack the human elements of the system, for instance through social engineering. The Systems Security Group at Northeastern is actively researching ways to detect and prevent attacks against existing systems, as well as designing new systems that are invulnerable or resilient to classes of attacks. But there is still much work to be done.

For their part, industry and government are not idle. In particular, the Payment Card Industry Data Security Standard establishes a set of requirements that must be followed by companies that handle cardholder information. This standard includes measures for attack prevention and detection, as well as guidelines for security incident response. It is important to recognize, however, that adopting these measures is in no way a guarantee that your credit-card information will not be stolen by cybercriminals. Rather, their purpose is to reduce liability when breaches do occur. Incidentally, Visa has removed Global Payments from the list of the Security Standard-compliant service providers as a response to the reported breach.

What does this incident mean for the average credit-card holder? Do you have any tips for how cardholders can protect themselves from fraud?

Most cardholders will probably not be affected in any way. For those whose card information was accessed as part of the breach, you will receive a notification from the bank that issued your card with instructions that you should follow immediately. Of course, you should not be held liable for the security failures at Global Payments.

The unfortunate reality is that no level of vigilance on your part can fully protect your card information from attacks such as the one that occurred at Global Payments. Regardless, it is very important to: a) regularly monitor your bank and credit-card statements and report irregularities; b) scan your computers and watch for signs of malware; and c) be careful how and to whom you divulge sensitive information. Best practices such as these will help to reduce the risk and keep your sensitive information safe