Why you should care about cyber security

Joseph Franell
Comment

As we have become more connected through e-mail, social media, and now through the "Internet of Things" (devices that talk to each other without human interaction), we have become more vulnerable than we ever imagined.

Hacktivists, nation state sponsored entities and cyber-criminals are actively targeting individuals, businesses and governments. Who are these criminals, how do they attack us, and how do we defend ourselves?

Threats come in three general forms. Hacktivists are focused on digital vigilante justice. Examples are the group Anonymous and the Islamic Jihad. Anonymous is a loosely associated group of hackers who attack government, religious, and corporate websites, mostly through distributed denial of service attacks (DDoS). In recent years, they are famous for targeting Israel, al-Qaeda and Donald Trump. The Islamic Jihad is famous for hacking Israeli surveillance drones, allowing them to see what the drones saw for at least two years before being discovered.

Nation state sponsored entities' main focus is twofold: espionage and causing physical damage. It is assumed that most governments participate in this against other governments. Just last year, ISIS (a nation state sponsored entity) was credited with attacks against the U.S. Central Command, Mountain View Telegraph, Newsweek, 54,000 Twitter accounts, France, and Global French TV network TV5Monde.

Finally, and perhaps of most concern to the majority of us, are cyber-criminals. These are the people and organizations that engage in identity theft, credit card fraud, tax return fraud, medical fraud, and corporate fraud.

For businesses, cyber-criminals are not just bad guys from Ukraine, Russia, and China; they may be members of the janitorial staff, vendors, visitors, and employees. Often, cyber-attacks begin with a physical breach either by an insider stealing information from the company's computers or a visitor/vendor installing a keystroke reading program or device on specific computers. Keystroke readers allow the criminal to see every keystroke you make on your keyboard. This allows them to get login and password information for various systems and websites. Wireless keyboards can be fairly easily hacked remotely (from just outside a building) which makes it even easier to get keystroke information.

Another common attack approach is social engineering, either in person or over the phone. Social engineers often pose as computer or IT support technicians and convince you to reveal your login credentials or give them remote access to your computer. Cyber-criminals also exploit known weaknesses in software configurations or software that has not been "patched" or updated.

Most home cyber-attacks come from wireless devices that still have their default passwords and through "phishing" emails. When you buy a wireless router or home automation device, it comes with a default password. Sadly, most people never change the default after they install the device. Default passwords are widely known and make it simple for hackers to access your home computer and network. Criminals have found ways to turn off alarm systems and even unlock doors.

Phishing emails look like they come from someone you do business with (bank, internet company, retail store, etc.) and often ask you to validate account information, change your password, or click on a link. Any of those actions can give the bad guys your password or download spyware onto your computer.

Ransomware attacks are becoming more and more common as well. Cyber-criminals gain access to a business or individual's data and encrypt it so that you can't access your data. They'll unencrypt it only after you pay them a ransom. Cyber-criminals mostly focused this kind of attack on individuals but are more often beginning to target enterprises. The Board of Water and Light in Lansing, Michigan, was a victim of a ransomware attack last month, and they had to lock down their entire network for more than a week while they purged and restored all of the impacted data.

Why should you care? Here are my top two reasons.

First, cyber-attacks cost money and we all bear the additional burden of those costs. For example, we pay more credit card overhead (interest and fees) on every transaction because companies have to recoup their losses. Secondly, cyber-threats to utilities and national security put our way of life at risk.

I've recently attended two briefings by leaders in this field, and both left me feeling nauseous and vulnerable. The bad news is that there is no way to absolutely protect yourself or your company. And many people and organizations do little or nothing to secure themselves, which makes them the easy and obvious targets for the criminals.

A long time ago, a friend told me a joke that went something like this: "You and a friend are walking in the woods when suddenly you are confronted by an angry bear. How fast do you have to run to get away?" The answer was: "You just have to run faster than your friend." Protecting yourself from hackers and cyber-criminals is much like that. You just need to make it difficult enough for them that they move on and attack someone else.

How do you accomplish that? Here are some practical tips that will help:

• Immediately change default passwords on wireless devices.

• Use strong passwords. Strong passwords are not easily recognizable words. They use a combination of upper- and lowercase letters, and special characters. Also, they are long. I am told that attackers, with all of the power of cloud computing at their disposal, can crack encrypted passwords of eight (8) characters in a matter of minutes (depending on the complexity of the password).

• Change passwords regularly.

• Use good virus, spyware, and firewall protection.

• DON'T EVER open emails from people or organizations that you don't know.

• DON'T EVER click links in emails or on social media if you are unsure of the origin.

• If a bank or other entity asks you to update information, don't use a link in an email to get there. Go to the company's website directly to do the updates.

At your place of work, make sure you have good policies in place and enforce them. Keep all of your software patched/updated. Limit access to your systems and educate your employees on cyber-security.

I liken the above to learning as a child to look both ways before crossing the street. Cyber vulnerability is just part of the world we live in. Taking steps to stay safe should become as natural as looking both ways before entering a crosswalk.

■

Joseph Franell is the CEO of Eastern Oregon Telecom, an internet and phone company based in Hermiston.

AP Photo/Matt York, File

Electricians install solar panels on a roof for Arizona Public Service company in Goodyear, Ariz.

GOP states benefit from shift to wind, solar energy

WASHINGTON (AP) — If there's a War on Coal, it's increasingly clear which side is winning.

Wind turbines and solar panels accounted for more than two-thirds of all new electric generation capacity added to the nation's grid in 2015, according to a recent analysis by the U.S. Department of Energy. The remaining third was largely new power plants fueled by natural gas, which has become cheap and plentiful as a result of hydraulic fracturing.

It was the second straight year U.S. investment in renewable energy projects has outpaced that of fossil fuels. Robust growth is once again predicted for this year.

And while Republican lawmakers in Washington have fought to protect coal-fired power plants, opposing President Barack Obama's efforts to curtail climate-warming carbon emissions, data show their home states are often the ones benefiting most from the nation's accelerating shift to renewable energy.

Leading the way in new wind projects are GOP strongholds Texas, Oklahoma and Kansas, home to some of the leading critics of climate science and renewable energy incentives in Congress. Republican-dominated North Carolina trails only California in new solar farms, thanks largely to pro-renewables polices enacted years ago under a Democratic legislature.

The most dramatic change has been seen in the plummeting cost of emissions-free wind energy, which has declined by two-thirds in the last six years thanks to the availability of cheaper, more efficient turbines. An annual analysis by the investment firm Lazard determined that wind energy is now the lowest-cost energy source, even before federal green-energy tax incentives are factored in.

"We are entering the era of renewables," former Vice President Al Gore said Thursday at the Climate Action 2016 conference in Washington. "It's a very exciting new reality."

Billions of dollars in private equity are going to construct massive new renewables projects, especially in the Sun Belt and Great Plains. Thousands of miles of new high-voltage transmission lines are also under construction to send power from the wind and sun from the sparsely populated areas where it is collected to the urban centers where it's needed.

Even with the surge in new projects, energy from such renewable sources as wind, solar and water accounted for only about a tenth of total U.S. power generation last year.

Still, the U.S. leads the world in wind energy with about 48,800 utility-scale turbines operating across the country, generating enough electricity to power about 20 million homes. By 2030, the Energy Department estimates wind will provide a fifth of the nation's electricity.

BRIEFLY

Free seminar on social media

HERMISTON — Business owners looking to improve their presence on social media are encouraged to take a class offered through the Hermiston Chamber of Commerce.

Take Your Social Media Marketing to the Next Level is Monday from 3-5 p.m. at the Hermiston Conference Center, 415 S. Highway 395.

The free seminar will provide tips on using photos and videos, what type of content to create and examples of how other organizations are utilizing social media for marketing.

To pre-register or for more information, contact kelly@hermistonchamber.com or 541-567-6151.

Mittelsdorf to speak at chamber

IRRIGON — Lisa Mittelsdorf, economic development director at the Port of Morrow, is the featured speaker during the upcoming Irrigon Chamber of Commerce meeting.

The no-host luncheon is Wednesday at 11:45 a.m. at Stokes Landing Senior Center, 195 N.W. Opal Place, Irrigon. The cost is $8 for chamber members and $10 for non-members.

For more information, contact 541-922-3857 or irrigonchamber@irrigonchamber.com.

U.S. hiring slowed amid tepid growth

WASHINGTON (AP) — U.S. employers pulled back on hiring in April, adding 160,000 jobs, the fewest in seven months, after a streak of robust monthly gains. The unemployment rate remained at a low 5 percent, roughly where it has been since fall.

Last month's hiring gain marked a drop from the average increase of 200,000 over the past three months.