CEO Worldwide Expert File

Cyber Ants Can Ruin Your Picnic

Written by Joe Orlando

Imagine. In the middle of the Super Bowl; in the middle of Wimbledon finals; as the top of leaderboard approaches the 16th tee; or during the overtime of the FIFA finals… imagine if suddenly, a score of kindergarten children made their way on to the pitch and began playing. Just one running free on the field would certainly disrupt the game would it not?

Your enterprise is a daily competitive playing field.
Every day – all day – there is a possibility that someone is trying to find a way to disrupt your business. The threats come in all sorts and sizes.

Oversimplified, there are three basic sorts of cyber attackers.

The first we will call "taggers." Like vandals and those who graffiti walls and buses, this sort of hacker merely wants to show off that they got into your systems. They want to be sure you know they were there. Shutting down email servers; encrypting your files and calling for a ransom; and flooding your servers to keep anyone else from reaching you.

The second sort we will call "wedding crashers." A great deal more subtle, these hackers enter your system and hope to go unnoticed. They stay and get to know everyone there… their passwords and access, for example. They hope to blend in and while some folks might wonder who they are and what they are doing in your systems, most will dismiss them as "somebody must know them," and think little more about them. Just like wreckers of a reception, they will eat, drink and enjoy the dance music while mingling as though they belong. They take data like a crasher may take a few of the prized wedding gifts. Some even stand to make speeches by authoring emails sent out in an official capacity. Eventually, enough people will begin to notice and curiosity will cause them to be outed.

The third sort is the most dangerous. We will call these "cat burglars." These are the most professional of the three and the most diligent. Much time and resources will be spent to "case the joint" – your enterprise. They want to know what are the most precious items you have and where you keep them. Most patient, many find their way in harmlessly enough and "wait in the pantry"

Written by Joe Orlando, iCEO # 7770

Contact us! **Phone: *+44 203 137 2581*** **Email: *search@ceo-worldwide.com***

Website: *www.ceo-worldwide.com*

CEO Worldwide Ltd - 9 Queen's Yard - White Post Lane, London E9 5EN, ENGLAND

until it is safe to come out and start their crime spree. They, most often, never want you to know they were there and will leave a door or window unlatched to enable them to return when they want to. Sometimes, they may not even take anything that you would notice – simply copy things and go. They covet things like personnel records for ID theft; customer information; vendor information; financials and more. A victim may never know the burglar was there, unless they made a mistake entering and/or leaving.

Despite all of this going on (and incidents on the rise) many executives and managers view security as an obstacle to efficient operations and a cost with zero return on investment. Further, security is most often viewed as "the IT department's problem."

The bold truth is that it is everyone's responsibility. Most of the entry points for attackers are directly with the assistance of unsuspecting employees. When a corporate network is used to do discovery on all servers and storage farms, it often finds, to its dismay, gigabyte after gigabyte of music files; video files; pictures stored on corporate assets that are personal in nature to the employee and either uploaded from a flash drive they inserted in their company PC or a download from their mobile phone or directly from the internet. The seemingly innocuous email offer and/or online deal that can't be past up, is often just what a hacker needed to get into your corporate systems.

No longer are these merely antisocial technology misfits in a dark room relentlessly tapping on a keyboard. There are well funded, professionally trained computer science teams – around the world – who have created and benefitted from this new form of internet piracy. The market will dictate the worth of what has been purloined so just take everything one can from you and someone – somewhere will be willing to pay for what a hacker took. An entire economy is operating on a sub-web that is driven by supply/demand and creative ways to take virtual assets and turn them into cash.

A little off track but the fact remains that everyone has to be sensitive to the need for security. Participate in the creation of security policies and procedures with empathy toward the best balance between operational excellence and a secure environment. A representative from every function should actively contribute to the Security Incident Response Team (SIRT) that comes together to manage and mitigate risk. Explore and identify the "Who? What? Where? When? And How?" regarding the breach and the ways to ensure it cannot happen again. The challenge is to ensure sensitivity is present to how actions in one area have impact on others. The cure should never come at such an expense to a function or functions as to hamper their ability to succeed.

It is an art form to facilitate and optimize the potential for the enterprise while delivering the most effective and comprehensive security. This requires all of the players on the team to play their part. When there is a breach, Legal may need to be involved to assist in managing the potential damage; HR may be needed to address the impact to employees; procurement and finance may be affected; and even if not directly impacted by the breach, all members need to be present to ensure the cure

doesn't do more harm than good.

The return? This question comes up a great deal. Do you recall the last time the power went out in the plant or in your offices? People went home, right? Generators are cost justified by loss productivity.

Now can you recall the last time the e mail server went down or the network was unavailable? Most people went home right? The loss is quantifiable. Now, if all the files on your shared servers were abruptly encrypted by an outside force so no one could access them… how long would it take before people went home? How much time would it take to shut the servers; reformat the drives and restore backup files to the drives? Not to mention the amount of work that has to be redone from the period of the last back up. If an entire department was unable to function for a complete day – salaries and expenses could be calculated easily enough but the work that would have been performed has a value. The cost to redo the work can be figured but the intangible still has value – opportunities lost; disappointed customers; brand impact; lost sales; and more.

Expectant parents pack a "go bag" and rehearse the fastest routes to the hospital. No differently here should enterprises have a Security Platform Plan; an Incident Response Plan; a Remediation and Recovery Plan and a Review of Existing Plans to ensure that this particular sort of breach (and those related) are included and addressed going forward… a well-defined AND DOCUMENTED cycle must exist.

So, the next time you see graffiti covered walls; suspect party crashers or try to figure out where to hide the coffee can with your emergency cash in it… here is hoping these feelings you will carry with you to ensure your organization's well-being.

About the Author: Orlando Joseph

Global Technology Executive with strong business and financial acumen. Strong ability to link marketing strategy and results directly to overall business strategy and company financial goals. Keen abilities to develop strategy from in-depth analysis of buyer and/or customer insights. Documented program development skills, from advertising to digital presence across all relevant marketing channels. Possesses excellent influencing skills and able to drive consensus. Able to recognize and articulate a future direction; provide strategic direction, and have the ability to direct global and localized products, brand, advertising and related specialties while managing budgets. A

CEO Worldwide Expert File

strong track record of new product development and demonstrated ability to forge strategic alliances with key partners. Accustomed to driving results and delivering return on investment.

Written by Joe Orlando, iCEO # 7770

Contact us! Phone: *+44 203 137 2581* Email: *search@ceo-worldwide.com*

Website: *www.ceo-worldwide.com*

CEO Worldwide Ltd - 9 Queen's Yard - White Post Lane, London E9 5EN, ENGLAND