Quanexus®
We make *IT* easy.

Corporate Account Takeover, Business Email Compromise & Ransomware

The Bad Guy is becoming more sophisticated in his attacks and more laser-focused on targeting your accounts

As cybercrime continues to rise, we are seeing a significant increase in Account Takeovers, Corporate Account Takeovers and Business Email Compromises. Account Takeovers are targeted to the individual, whereas Corporate Account Takeovers and Business Email Compromises are targeted to businesses across all industry sectors. While technically these are all different, for this article I will be using these terms interchangeably.

There is no good news here but by implementing some basic IT controls, you can greatly reduce the risk of being affected by these threats.

Although the focus of this article is about Account Takeovers, Ransomware is still a huge threat. The same protection controls mentioned in this article apply to protecting your network against ransomware and most cyberthreats.

How are criminals being successful?

There are typically two ways the criminals can succeed with taking over someone's account. The first method is through social engineering, and the other is by purchasing information being openly sold on the Internet and the dark web.

Social Engineering

Social engineering is the art of getting someone to do something that they would not normally do. If I asked you for the user ID and password for your bank account, I would hope you would not give it to me. If I disguised a website that looked just like your bank's website, and I sent you an email that looks like it legitimately came from your bank, you might click on the link in that email and go to my disguised website. Once at my website, you would enter your user ID and password, and I would say thank you! After I got your user ID and password, I would send you to the real website and you would have to log in again and proceed to do whatever you needed to do. This is happening all the time! The criminals are getting smarter at crafting emails and bogus sites that look and feel legitimate.

Account Credentials

The other method is to simply buy lists of stolen credentials. These lists typically include a user ID and password. You might wonder where these lists are coming from and if you need to be concerned. The answer is yes, you should be concerned. As you watch the news and read all the articles about big companies being breached, there are often user IDs and passwords stolen as part of the breach. The biggest breach to date where user IDs and passwords were stolen, was the Yahoo breach, which affected over one billion users. To put this number into perspective, there are about 325 million people in the United States.

A third method, which only takes a little more work, is to create some cool looking websites offering content people would flock to. Once you have an audience, you promise even better content, but require users to create a free account to access new, very cool content. The word free is a little misleading in this context. When the user creates their free account, the cost they paid is they gave the owner of the site their user ID and password.

Password Reuse

Two of the methods mentioned above take advantage of and illustrate the principle of password reuse. Password reuse, refers to the act of using the same password for multiple accounts. As a policy, companies should not allow users to use a password that they use for personal accounts. From an individual's perspective, it is difficult to manage a lot of passwords. At a minimum, everyone should at least have a few unique passwords.

Separate passwords should be used for on-line shopping accounts, and banking accounts. You should also have a password to use for low priority accounts that if breached, would not cause you any harm. If it is challenging for you to manage all your passwords, consider a solution such as Keepass or Lastpass.

Two or Multiple Factor Authentication (2FA, MFA)

I will be using 2FA and MFA interchangeably throughout this article. Another way to prevent an account takeover is by using multi factor authentication. Multi factor authentication requires two out of three items to login/authenticate to your account. The three items are: something you know (password), something you have (a token), or something you are (biometrics). Obviously, something you know are items such as a password or pin code.

Something you have is typically referred to as a token. Tokens come in two varieties. One is a physical device with 6 digits that change every 60 seconds. The other is an application that runs on a smart phone with a six-digit number that changes every 60 seconds. Something you are is a biometric. The most common biometrics for authentication are finger prints or a retina scan. If you are the owner of a late model iPhone, these devices now include facial recognition, which is being implemented as single factor authentication.

Real-Life Stories

Up-Front Fraud

A board member of a financial institution was building a new house. **They emailed the financial institution to wire transfer funds to one of the suppliers that needed to be paid up front.** Everything looked and felt legitimate. As a precaution before the transfer was initiated, because of their training, they called the board member to verify that the transfer originated from him. **This was a case of fraud**; the board member's personal email account was taken over by the criminal.

Stolen Credentials

A new credit card was issued to a non-employee of a company. The owner of the company had several credit card accounts, both personal and business. As a convenience, banks allow users to link multiple accounts to one user ID. The owner linked their personal account with the business account, and the owner used their personal email address as the account name for the bank. **Through social engineering, the criminal acquired the owner's user ID and password.** Once they had that information, they **requested a new card** to be created for someone that did not work in the organization.

Costly Key Logger

An organization had a fraudulent $280,000 payroll created. **The criminals had social engineered the bookkeeper and gained full access to her computer.** Once they had access to the computer they installed a key logger. **From the key logger they could determine the credentials to log into the bank, create 120 new employees and generate a $280,000 payroll to pay them.** There were many things that were not properly configured in this environment. One of the financial controls the company had is, they check their checking account balance each morning. The morning after the transfer, they quickly noticed this issue and put stop order on the issued payments, but it was too late to stop all of them. **The organization ended-up losing close to $90,000.**

Real-Life Stories (cont.)

Owner Imposter

A request for fund transfer to a new vendor. The accountant in a small business received an email from the owner of the company (who was out of town). **The email had a request to setup a new vendor and wire transfer funds to this company for product.** The email also stated that the owner had poor cell phone coverage where he was at, and if they needed him they could call later in the day, but it was urgent to get the funds transferred right away. The accountant at the office was shaken by this email. They called Quanexus as they suspected this might be fraud, but she wasn't sure. **It turned out to be fraud.**

Email Takeover

Another wire transfer story. **A financial institution received an email requesting a wire transfer.** It all seemed legitimate, but just to be on the safe side, they sent an email to someone else in the organization to verify that the request was valid. The financial institution received a reply from this other individual and proceeded to transfer the funds. **This was fraud.** The criminal had compromised the company's email system, and the response from the other individual was from the criminal, using the compromised email system. **This is why out of band verification is important.**

Everyone believes it won't happen to them or their organization, but the reality is it can happen to anyone at any time.

92.4%

of malware is delivered via email.

- Verizon 2018 DBIR

Everyone believes it won't happen to them or their organization, but the reality is it can happen to anyone at any time. Organizations need to have their employees trained and have the proper controls in place to identify potential issues. Additionally, there needs to be controls in place to validate the credibility of requests. There are several ways to validate credibility.

Validating Credibility and Dual Control

Out of band communications is a good way to verify that a received request is credible. You should never use the same technology to validate credibility that was used to generate a request. Typically, requests are received by email, so to validate this, you should call the individual to confirm it is legitimate. By having a second person who knows of the request and is required to validate it represents the principle of dual control. If the request was called in there should be some passcode required to confirm the request is legitimate.

Bank Account Controls

Financial institutions offer several solutions/products to enhance the protection of your checking accounts and ACH transactions. One of the popular controls requires someone from the organization to log into the bank account daily and approve all ACH transfers. If they are not electronically approved they will be canceled. For checking accounts, a popular option allows you to log into your account daily and permits you to put a stop on any check transaction that is not authorized. The default on this solution is, if no action is taken, the payment is processed, unlike the ACH transaction, that requires an action to allow the transaction.

Keyboard Loggers and Social Engineering

I opened this article describing the two most common ways criminals are stealing your credentials. Number three on the list involves the use of a key logger. A key logger is just what it sounds like, it is a tool that logs the keystrokes on your keyboard. In the scenario of the $280,000 payroll, social engineering was used to compromise and install a keyboard logger. As mentioned, there were many things that had been neglected in this environment. If there would have been a good security stack installed, the computers would not have been compromised.

How do you keep your organization protected?

Whether you are a small business or a large enterprise, the best way to keep your organization protected involves a layered security approach. Quanexus has developed our Q-Stack which provides a comprehensive approach to network security. The difference between attacks focused on large enterprise organizations vs small and medium sized business is, no one is waking up in some foreign country looking to hack most small and medium sized organizations. The criminals don't want to work hard, and why should they. There are many organizations, like the one with the $280,000 payroll stolen, who don't take security seriously and they are the low hanging fruit criminals are looking for.

By implementing a security stack, you will be moving your organization from low hanging fruit to a position much higher on the tree.

What does a security stack include?

POLICIES & CONTROLS

At the top of the stack are policies and procedures. These set the ground rules for many items such as, password length and how frequently passwords must be changed. The principle of least privilege, back policy, and much, much more.

FIREWALL

Next Generation Firewalls (NGFW) are extremely effective at protecting a network. NGFWs include: an anti-virus engine, intrusion detection and prevention, application filtering, DNS filtering and more.

SECURITY AWARENESS TRAINING

Users need to be aware, especially when it comes to social engineering. Other topics for security awareness training are: how and who to report a potential incident to, not to share passwords, not to overshare company information on their personal social media sites, and much more.

ANTI-VIRUS/ MALWARE

It is important to have a managed anti-virus/malware solution in place. The key word here is managed. It is not good enough to simply turn on automatic updates and assume it is working. It is very likely that if an update starts at a time when things are busy, a user might disable the update process. They may have had good intentions to turn the AV solution back on when they complete their tasks, but often, because they are busy, they forget. Now you have an unprotected, potentially vulnerable system on your network. A managed solution does not allow the end user to disable the solution and provides reports indicating the status of the solution. So, if there is an issue with the updating process, it can be quickly remediated.

PATCHES & UPDATES

Operating systems and programs contain hundreds of thousands, if not millions lines of code. They suffer from two problems: one is stability, the other is vulnerabilities. Patches to operating systems and programs remove the type of vulnerabilities that would allow a criminal to install malicious code, such as ransomware or key loggers on your systems.

BACKUP

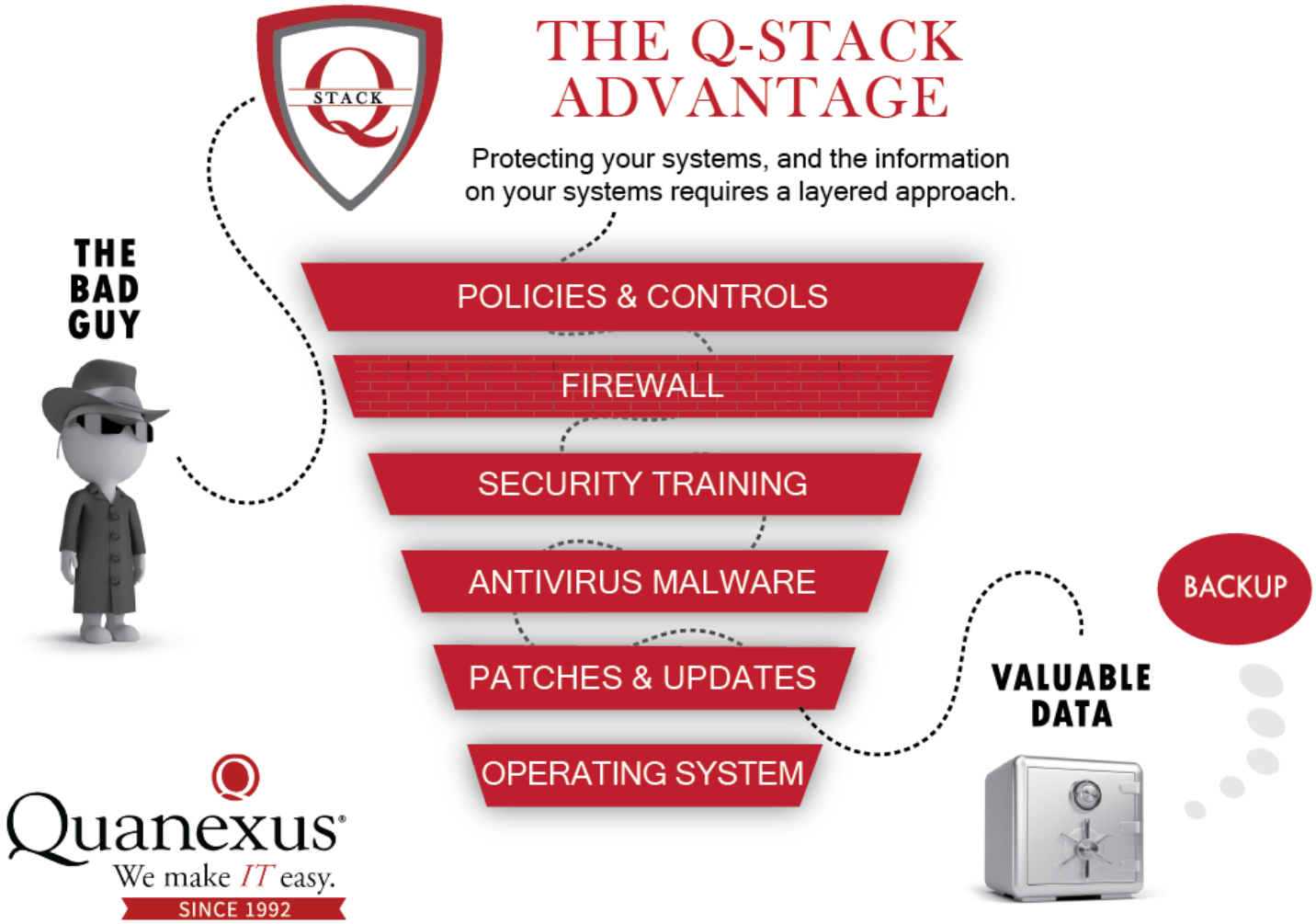
As part of a good security stack there must be a rock-solid backup solution. It is possible that after implementing all the best security controls, your organization may still experience an incident where data is lost. In that event, the only thing that can be done is to recover your data from a backup.

A Word About Data Loss VS Data Theft and Breaches

Data loss can occur due to non-cyber issues or events. These events range in magnitude from lost or stolen devices to data corruption or equipment failure. While these are security type incidents, if the lost or stolen devices were encrypted, it is not considered data theft. Data theft is a serious issue. This means the organization has lost control of potentially protected data and the theft may constitute a breach. Many states, including Ohio, are breach notification states. The definition of “breach” is specific and defined by each state.

There are specific reporting requirements which vary by state. The word breach should never be used by anyone in a company (especially senior management). If you suspect your organization may have experienced a breach, the proper term to use is “incident”. If pressed for a statement, it should be nothing more than “we have experienced an incident and we are investigating it”. If a breach is suspected, you should work with an attorney who specializes in privacy or cyber law.

The best way to protect your organization from any type of cyber incident is to have a layered security stack, such as **Quanexus Q-Stack**. Our stack is a comprehensive layered approach as illustrated below.



Quanexus.com
571 Congress Park Drive, Dayton, Ohio 45459
937.885.7272 | info@quanexus.com