Kaseya® White Paper

Five Ways to Reduce the Risk of Cybercrime to Your Business

Kaseya

THE IT MANAGEMENT CLOUD COMPANY™

The Internet has become an essential component for businesses of all sizes, and is necessary for them to operate and compete. It allows access to a variety of innovative tools and resources that help reduce costs and increase productivity. It is becoming easier than ever before for businesses to store and access their most sensitive information from almost anywhere, on almost any device, and without the need to spend thousands on IT equipment or the associated costs to maintain it.

The world is changing, and so too is the threat landscape. The growth in information technology is attracting more and more cybercriminals looking to steal the valuable corporate data produced and consumed with this technology. From intellectual property to protected health information, from digital financial assets to trade secrets shared within the corporate network, attacks to the vital information that drives our businesses are becoming more commonplace, and the associated risks also increase as cybercrime becomes more profitable and prevalent. In fact, the risks and costs of cybercrime continue to increase each and every year.

In October of 2014, the Ponemon Institute released their global report on the cost of cybercrime[1]. They found that over the past year, the mean cost of cybercrime had increased by over 10%. Their results also demonstrated that cybercrime and cyberespionage are problems for businesses of all sizes and industries. No one is immune.

On March 21st, 2013 the United States government held a public meeting about "Protecting Small Businesses Against Emerging and Complex Cyber Attacks".[2] In it, the expert testimony focused on how small businesses are being impacted greatly by state-sponsored cyberattacks from foreign nations. This isn't just a problem in the U.S., nor is it a problem for small businesses alone. Through the ever connected world of the Internet, the threat landscape of cybercrime is equidistant to all businesses, putting us all at risk.

While some still naively cling to the belief that it will never happen to them, there is a paradigm shift around security as businesses of all sizes embrace the cloud and extend their access to valuable resources. Everyone is beginning to see the inherent value of information security.

Do businesses really fail after a cyberattack?

In the past few years there have been a string of cyberattacks on high profile companies that demonstrate a real threat out there. However, if you look closely at many of these affected companies you will see that they have weathered the storm after the breach, in many cases with demonstrated increases in business and stockholder value. Often this is because of the financial and business resources that organizations like TJ Maxx and Heartland have at their disposal. But what about the businesses which don't have such resources available, or for that matter, what about the long term damages which we are only now beginning to see?

"Through the ever connected world of the Internet the threat landscape of cybercrime is equidistant to all businesses, putting us all at risk."

1 https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf
2 http://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=323427

According to research from Symantec[3], 40% of all targeted cyberattacks were directed at SMB companies of less than 500 employees, while the remaining 60% of attacks were aimed at companies with 500+ employees. Further, McAfee released an online threat report at the beginning of 2011 that predicted some of the biggest threat loopholes would jeopardize more and more businesses through attack vectors like mobile phones and personal tablets. Users rarely consider security when they're using these sort of devices, yet they use them to connect to critical business systems and information all the time. End users are always the greatest risk to IT security, and those larger businesses have more, vulnerable end users than any other.

Businesses can and do fail after cyberattacks. Companies like CloudNine, BlueFrog/Blue Security Inc, Code Spaces, DigiNotar, and Distribute.IT all demonstrate how cyberattacks can affect business, with all of them closing a short period of time after their attacks. That is why it's critical that all businesses assess their risks, document the processes to handle them, and then apply safeguards to address them.

If you take anything away from this, just remember that it really isn't safe out there. While you won't be able to defend the digital divide from all things malicious and hostile, you can take precautions and put in processes to assist you in reducing your risk of becoming another cybercrime statistic. This includes strategies for backing up data and recovering from failure, having an incident response plan on how to address such acts, and investing in the right technical safeguards to mitigate the risk of cybercrime to an acceptable level.

What can be done to mitigate the risk of cybercrime to my business?

While there are an innumerable number of ways you could improve your business's information security posture, for the sake of brevity let's shorten that list to the methods which often provide great benefits. Here are five ways that you can help your business reduce the chance of being victimized by cybercrime.

Task #1: Regularly audit your environment

Does your company perform regular internal audits? It's a simple enough process, however, many people consider them unnecessary, or too cumbersome. Often, audits are left unfinished, and even those who complete audits often consider them useless, or are unwilling to act on the results. In actuality, a properly run audit can be one of the most useful measures of an organization's IT security. Still, many find that the time requirements of an audit are too demanding. As such, automating the process is highly recommended. The following presents an example of how this could work in practice.

If you have a baseline for what the network should look like, you could then strike those healthy results from the results of further automated hardware audits. That would leave you with a list containing changes to the network each time it is audited. If a user hooks up any device to their system, like a modem or a hard-drive, you would be able to see this with the audit. If you have a heathy baseline audit of the network, then any changes to the network could be found. If some of your users set up an unapproved wireless access point, then you'll know about it. A good remote monitoring and management (RMM) toolset will allow you to automate these audits, and will be able to do most of the heavy lifting for you.

Similarly, password auditing allows you to track which people are using weak, old or otherwise out of policy passwords. If your users are assigned individual logins for administrative purposes, yet all administrative logins are recorded as being from a single account, then there's something improper going on. You could then lock that administrator account and the systems logged in with it, and deal with those users accordingly. A good password change management process combined with a strong password management system can significantly improve your ability to address policy violations and improve access accountability and security.

Knowing your own systems is critical for maintaining a reasonable degree of IT security; if you don't

3 http://www.symantec.com/connect/blogs/targeted-attacks-and-smbs

"Companies like CloudNine, BlueFrog/Blue Security, Inc., Code Spaces, DigiNotar, and Distribute.IT all demonstrate how cyberattacks can affect business, with all of them closing a short period of time after their attacks."

know your systems well, how are you going to protect them? Sun Tzu explained it best when he said "If you do not know your enemies nor yourself, you will be imperiled in every battle." If your RMM solution can automatically handle this information gathering for you, then the benefits are that much more pronounced.

Task #2: Use stronger authentication

IT security has always been, and will continue to be, dependent upon validating identities requesting access to resources. Many industry experts agree that we cannot continue to rely on passwords alone to authenticate users, especially remote ones. Ensuring the strength and security of the authentication method being used should be of the utmost importance.

Whether it's an administrator managing an IT system, or an end-user accessing sensitive corporate files, validating users' identities is vitally important. Is it really Alice in accounting, or is it Oleg from Romania pretending to be Alice using her stolen credentials? If you don't think this could happen to you, think again. Evidence from Verizon's Data Breach Report[4], and Mandiant 2014 Threat report[5] demonstrate that this is a common occurrence, with Mandiant reporting that compromised ID's were used in 100% of the cases they investigated, and with Verizon reporting the same for 70% of the businesses they investigated.

There are two ways to solve this problem. One method involves automation, which we will cover in the next section. The second method is exactly that, a second method. Using a username and password is what is known as single-factor authentication -- something you know. When a second method of authentication is added to that, the confidence in the authentication is much higher. This is referred to as either "second factor" or "multi-factor" authentication.

There are three broad categories of authentication factors: knowledge based, possession based, and inherence based. Knowledge based authentication requires that users prove they know a secret combination, like a password, PIN, or pattern. Possession based authentication requires users prove they possess items that only they should have, like a physical key, their smartphone, or an ID card. Inherence based authentication tests that a user physically is who they claim to be, often through some sort of biometric reader. If an authentication system uses at least two of these three factors, then it can be considered a multi-factor authentication system.

Here's an example of how this could work in practice.

Some criminals attempt to gain access to a system that requires multi-factor authentication. They manage to get the password and attempt to sign into the system, but are unable to pass the possession based test. As a result, they cannot gain access, the logon failure is reported, and the system automatically locks that account, preventing any further access attempts.

Multi-factor authentication, when properly implemented, makes it nearly impossible for people to log into systems for which they aren't explicitly provided access. This effectively mitigates much of the risks inherent in traditional single-factor authentication. If you rely on passwords alone to secure your systems against attackers, then your security could be woefully inadequate.

Task #3: Strengthen weak security through automation

Automation as a security measure can be easily understood, yet can also be difficult to implement without planning. Think of it this way, if a cybercriminal is looking to gain access to a system through the use of a compromised account credential, then making those credentials difficult to access makes their job more difficult.

The key to automation as a security measure, is making your account credentials dynamic and more difficult to track down. That raises the question though, what makes a password dynamic? Consider this, if your password is static, then with enough attempts over time it can be guessed by an attacker, thus compromising your identity. If the password changes every few minutes from one

"Multi-factor authentication, when properly implemented, makes it nearly impossible for someone to log into a system they aren't explicitly provided access to."

4 http://www.verizonenterprise.com/DBIR/2014/
5 https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

secure password to another, then it becomes statistically improbable to guess, leaving virtually no chance that an attacker gets the correct password before it changes again.

How can users keep track of a password that changes so frequently? It's simple... make it so they don't need to. Earlier we discussed the use of multi-factor authentication. Such a system can automatically handle this for you. A password may be generated by a token on the person, used once, then expired by the automated system, thus minimizing the time-frame a password is valid. However, this may not be practical for every system you need to access where a traditional password may be more commonplace or required.

This is where automation as a means of security comes into play. You can automate the changing of passwords after use so that even if an adversary did gain access to the password through the vile and villainy of the Internet, the window of exposure is significantly shortened by having the credential changed soon after use. So the criminal element ends up holding the old password to the system, which is no longer in use. A good password management system which supports password change automation can do this for you. Even better, if it supports Privileged Identity Management (PIM) this becomes even easier for your users, as they won't need to fret about anything. It's all done for them automatically, and they won't even notice the updates.

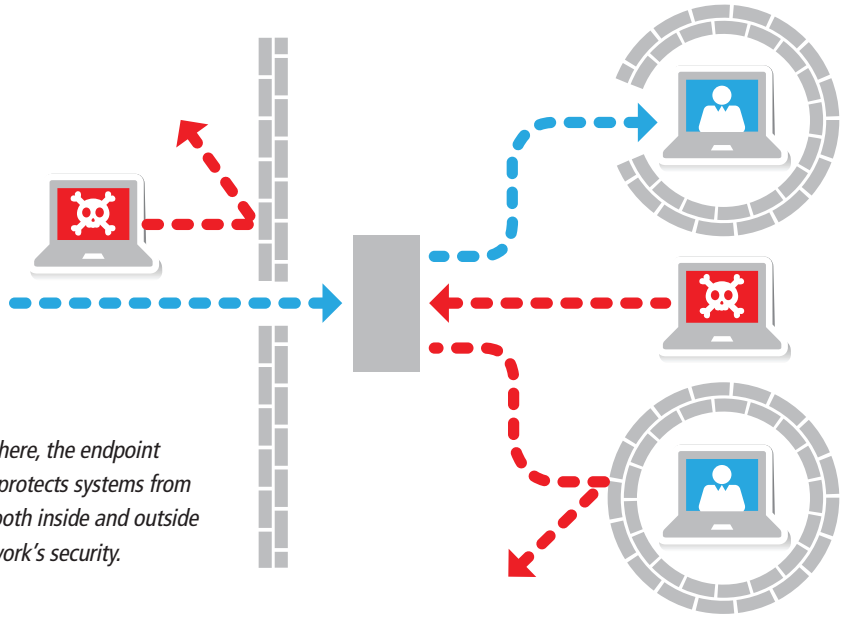
Of course, automation can also mean finding more meaningful ways to facilitate the sign-on experience without having to even know or use a password. Through a combination of stronger multifactor authentication and access to single sign-on technology, authenticated users can gain access to systems and services without having to do anything past clicking an icon to sign in.

With automation, end users don't know their own passwords, thus eliminating the risk of them knowingly or unknowingly giving them away, and the passwords are continually changing behind the scenes when they are needed and used. This means that the risks of social engineering and password cracking are effectively mitigated, thus thwarting the activities of cybercriminals, all while making it easier for authorized users to gain access to the systems they need.

Task #4: Secure your endpoints

Endpoint security serves to protect systems from threats that penetrate past the network security boundaries as well as threats which come from within the network, like a compromised personal, BYO system.

In the market, endpoint protection solutions are often labelled Advanced Endpoint Threat Detection. In the consumer environment, these solutions are the extent of the protection people buy. In a corporate environment, it is meant to supplement network security.



As seen here, the endpoint security protects systems from threats both inside and outside the network's security.

"With automation, endusers don't know their own passwords, thus eliminating the risk of them knowingly or unknowingly giving them away, and the passwords are continually changing behind the scenes when they are needed and used."

As seen in the diagram, endpoints are vulnerable internally because holes are intentionally created in the network security perimeter to allow internal and external business users access to resources. Endpoint security serves to augment network protections, improving the systems' ability to defend itself where network security is insufficient or inapplicable.

Additionally, securing endpoints helps to mitigate the risk presented by mobile systems. (By mobile, we mean any system which connects to networks both inside and outside the protected/trusted network perimeter.) With the availability of wireless hotspots and cloud computing, teleworking is more popular than ever before and can greatly improve user productivity. Unfortunately, it can also increase the risk of infection. If a system is compromised while it's off network, it can act as a carrier for the infection, aiding threats past network security. As endpoint security protects the system locally, the risks posed by those "mobile" systems are significantly decreased.

No security system can offer absolute protection, so we must take a defense in depth posture to safeguard systems and corporate information. Without endpoint security, attacks originating from within the network and those which breach the network perimeter would be uncontested. The risks of both internal and external threats can be significantly reduced with endpoint security.

With so many endpoints to secure, manually managing these systems is a never-ending job. Attack profiles are constantly changing, so updates to these systems must come frequently and automatically. Due to this, being able to automate the installation and maintenance of these systems through an RMM system is incredibly valuable.

Task #5: Educate your users

You can roll out the best security software and hire the best IT security staff money can buy, and it will change nothing if your employees aren't safeguarding company information and resources. Remember that absolute security is a myth; with enough money and motive anything can be breached. History has shown that this is often done through the weakest link… which is usually the people.

A bank vault is only secure if it's locked shut by bank personnel; if it's left open then the walls may as well be made of paper. When you're securing your company's IT infrastructure against cybercriminals the same applies, and the people who most often leave that door open are your end users. They have legitimate access to the resources, systems, and services which criminals are after. If staff are reusing their AD credentials across insecure domains and installing programs with no heed to the risk of being compromised, then there's not much that can be done to protect the information they can access. This is why education is so important to combine with the other four tasks.

Though many organizations attempt to use technical controls in place of user education, in the end, technical safeguards are meant to support users and management in combination with user education. This is why user education is one of the most potent ways to reduce the risk of cybercrime. There are innumerable topics that could work for these lessons, and any lesson end users learn can potentially help to mitigate risk. Just keep in mind that how you pass along that information is nearly as important as the message itself. If a presentation is unclear, uninspiring, or lacks evidence of its importance, then people will ignore and forget what they were told, it's just that simple. That's why lessons which are honest, relevant, and memorable are ideal when you're trying to pass on important lessons.

One great way to accomplish this is by using examples which have recently received significant media coverage. People remember events like the October 2014 Dropbox "hacking" incident, where username and password combinations were collected on other websites and used to access Dropbox accounts. Work a timely event like that into a lesson about why reusing passwords is a dangerous practice.

Just to reiterate, the most important thing when you're educating end users about IT security is that you do the topic justice, and do it regularly. Help staff stay informed so they can stay vigilant.

"You can roll out the best security software and hire the best IT security staff money can buy, and it will change nothing if your employees aren't safeguarding company information and resources."

Going Forward

Once you've educated your users, make sure to remember…"hey, they're only human." Then look back at the other four points and strengthen them as you realize making it easier for the user to do their job while making it difficult for the cybercriminal will add more value than education alone. That's not saying user education is not important, but that it's only one piece of a bigger puzzle.

When you consider the risk of cybercrime, the benefits of risk mitigation become quite obvious. Unfortunately, the work needed to effectively accomplish all of these tasks can seem like an equally daunting task. That's where Kaseya can help. While we won't train your users on IT security's best practices, we can ease the processes of auditing, automating, authenticating, and securing endpoints. Kaseya offers solutions for each of these challenges by automating them and providing a single management interface and reporting dashboard.

About Kaseya

Kaseya is the leading provider of cloud-based IT management software. Kaseya solutions allow Managed Service Providers (MSPs) and IT organizations to efficiently manage IT in order to drive IT service and business success. Offered as both an industry-leading cloud solution and on-premise software, Kaseya solutions empower MSPs and mid-sized enterprises to command all of IT centrally, manage remote and distributed environments with ease, and automate across IT management functions. Kaseya solutions are in use by more than 10,000 customers worldwide in a wide variety of industries, including retail, manufacturing, healthcare, education, government, media, technology, finance, and more. Kaseya is privately held with a presence in over 20 countries. To learn more, please visit **www.kaseya.com**

Kaseya®

THE IT MANAGEMENT CLOUD COMPANY™