PROTECTING YOUR CORPORATE EMAIL

10 IMPORTANT QUESTIONS THAT YOU SHOULD KNOW THE ANSWERS TO

WHITEPAPER

September 2016

Vircom

www.vircom.com

10 IMPORTANT THINGS

Sony. Ashley Madison. Home Depot. Target.

What do all these companies have in common? Well, other than their uncanny ability to attract the attention of middle-aged men, there's something big — they've all been victims to some of the worst corporate hack attacks.

Picture this: customer, supplier and employee information thrown to the wind, millions of dollars spent recovering lost records and fallout from reputational damage for years to come. For any business owner or IT employee, this doubtlessly evokes images of four horsemen, mushroom clouds, and fire and brimstone. Melodramatic, sure, but data breaches really can spell the end for an organization. And all it takes is one email with a malware virus or a clever phishing scam to do it.

Email security software has never been more vital. Recently, rising email security start-up Virtu secured $29 million in funding. If Silicon Valley backers are investing in it, you should be too. That said, email security can seem huge and daunting, particularly with so many stories of doom and gloom constantly in the news. We never want you to fall victim to hackers or your own paralysis about getting started. That's why we've put together the answers to 10 of the most commonly questions about protecting corporate emails.

Read, enjoy, encrypt!

QUESTION 1:

DO I ACTUALLY NEED TO PROTECT MY EMAIL?

Unequivocally, yes, According to the Radicati Group, most of us send and receive 122 business emails every day, for a total of over 100 billion corporate emails sent daily, globally. That's a lot of important, valuable information.

Despite our growing fondness for social media in our personal lives, in professional settings email dominates all other forms of communication for ubiquity and convenience. When emails were originally developed, the mentality was more: "send now, secure later."

Things have changed.

Hackers now know that corporate emails are treasure troves of data, and personal and financial information — whether it be yours, your customers' or your business's. According to the Ponemon Institute, the average cost of a data breach in 2013 was just over $5.4 million. Could you afford that?

Hackers are also getting sneakier. Abdicating their old Nigerian royalty mainstays, they now can use something as simple as your phone number and SMS to hack into your email now. Once they've dug into your data, they can sell it to the highest bidder or put it out into the world. Not to make you paranoid, but with increased users and devices to access email on (smartphones, tablets, desktops, laptops), there have never been more opportunities for hackers.

Take for instance the recent email leak of the Democratic National Committee (DNC) by the hacker Guccifer 2.0. According to the Washington Post, had the DNC encrypted their communications, Hillary Clinton may have been spared the resulting embarrassment and voter loss. Don't follow her lead and get "trumped" by hackers.

QUESTION 2:

HOW IMPORTANT ARE THESE LAYERS OF EMAIL FILTERING?

If you've seen one email security provider site — you've seen them all. All the email filtering layers, that is.

For example:

- Bayesian filtering
- Snowshoe spam filtering
- Fast flux detection
- RBLs, DNSBLs, SURBLs
- Connection-Level blocking
- Sender reputation
- Anti-phishing
- Content filtering
- Rules-based filtering
- SMTP header analysis
- Anti-virus filtering
- Heuristics engine
- Scripting
- Attachment scanning
- Foreign language filtering

While the list may be long, the short answer to whether more layers are necessary and an indication of performance is: probably not. Vendors will try to convince you more layers means more complex technology to justify a higher price. Don't fall prey to the bells and whistles. You really need to focus on three key questions:

- How much of "bad" stuff does it block?
- How bad is the stuff it lets through?
- Does it catch stuff it's not supposed to i.e. "good" stuff?

You won't get the answer to those questions on a laundry list of filters. The only way to find out is trying the email filtering solution on your own email stream. Make sure your solution submits itself to independent performance tests independent performance tests and review the results. Independent tests are objective and the best won't even tolerate a single False Positive (a "good" message that was caught).

Email stream security is also subjective. We don't all receive the same kind of malicious messaging or spam. Your stream is different than someone else's, so a solution that works for another company might not work for yours. A good solution can tweak and customize its filters to meet your needs, and a good provider will offer to do that customizing for you. They will also provide periodic reviews to ensure the solution is still performing and meeting your individual productivity and security needs.

QUESTION 3:

IS ENCRYPTION IMPORTANT FOR EMAIL SECURITY?

If you don't want your emails to be an open book, you need encryption. Core email protocols do not include encryption; they're sent in clear text, which makes unencrypted emails easy reading material to hackers with moderate skills and tools. For most users, a basic packet sniffer will suffice.

There are three basic encryption choices:

1. You can encrypt the channel over which emails are sent
2. You can encrypt the emails themselves
3. You can do both

For non-tech users, the differences under the hood between these encryption options become confusing quickly.

Here's a cheat sheet to make it more digestible:

- Encrypting the channel uses **Transport Layer Security (TLS)** which comes in two major forms: Forced and Opportunistic
- **Forced TLS** is rigid and will only accept connections from servers that support TLS
- **Opportunistic TLS** is more forgiving and allows messages to be sent if TLS is not supported
- Disregard **Secure Socket Layer (SSL)**; it's been cracked and is considered obsolete
- Encrypting the message itself involves **S/MIME or OpenPGP**, and uses two different mechanisms: Push and Pull
- **Push:** Clients are able to encrypt and decrypt the message and manage keys
- **Pull:** Clients are typically web-based and the user signs up and in one time to a secure website over https to retrieve the contents of the message
- Pull email encryption has become the more popular of the two due to ease of use

If you encrypt both the channel and the message, be prepared for a lot of configuration overhead. If you're only going to use one, go with encrypting the message. Encrypting the channel is incomplete protection, doesn't secure the contents of the message and leads to many rejections.

There's the trade-off though: security or usability? Encryption poses a key usability problem, with the most secure system being locked up and basically unusable (i.e. Forced TLS), and the most functional, open system being completely insecure. Fortunately, it's a spectrum. It's up to you, the user(s) of the system, to establish which end you'd like to be closer to.

Encryption is complex stuff. Nowadays, progress has been made to turn "encryption key management" from a headache to an afterthought for end users with more advanced systems. Basically, the tech sweats so you don't have to.

While there are many vendors of encryption solutions, the pool of developers and publishers is surprisingly small. This allows them to hike the prices on their solutions. It may sometimes seem steep, protecting your data is an investment. According to Ponemon Institute, the cost per record in a data breach is now $154 USD — up 12% from the year before. We'll give you a second to process that and call your vendor.

QUESTION 4:
DO I NEED AN ANTIVIRUS WITH EMAIL FILTERING?

If you want complete protection, yes. Fortunately, it's usually a 'two birds, one stone' situation: most email security developers also produce antivirus software and include it in their solutions.

Sure, most emails containing viruses will get caught by anti-spam solutions. But do you really want to gamble with your data security — and, potentially, your reputation? Your safest bet is going with an email security solution that at least has an extra scan for viruses. Double your chances by going with an option with two antivirus engines! Before you go all-in though, there are a couple things you should know.

GO WITH QUALITY

First is the suggestion to pursue a recognized publisher that has a track record of quality and performance. Many anti-spam vendors will only integrate the free Clam AV software. Yes, it's cheaper in the short term. No, it's not enough to protect a business.

AND SOME QUANTITY

The second thing you should remember is: one anti-virus engine is good, two anti-viruses engines is better, three anti-virus engines and you're probably being ripped off. No single engine is perfect. It's a certainty that at least one virus will get through if you only have one layer of protection. Adding a second engine from a different, reputable, top-rated publisher decreases chances of something slipping through and increases security. (Side note: Make sure you're not being duped with a second engine that just turns out to be free Clam AV. You want

quantity and quality.) Why not have three? At that point, it's diminishing returns. Chances are you're paying a lot for little added security.

THE COST OF SAVING MONEY - AND FACE

Our third point is cost. Having dual antivirus engines from top-rated publishers is pricey. Ultimately, it's worth it though. There's a saying: "You have to spend money to make money." When it comes to email security, it's more like, "You have to spend money so you don't lose *all* your money — and your client's money and probably your business." Doesn't have quite the same ring to it, but you get the idea.

And we don't just talk the talk — at Vircom, we walk the walk by we including the industry's consistent top two rated engines: Avira and Bitdefender.

QUESTION 5:
HOW MUCH SHOULD I BE PAYING FOR ANTI-SPAM FILTERING?

Let's start with how much *could* you be paying? That's easy: $0. Go with a free solution like SpamAssassin or Clam AV. Will it block a lot of spam and malware? Absolutely! Will it block it all? Not by a long shot.

You save in short-term costs by going with free offerings, but as you've probably gathered by now, when it comes to email security solutions, you get what you pay for. Remember: time is money, too. If you go with a free solution, you will pay a fortune in the long run once you factor in the additional resources spent monitoring, tweaking and adapting each day, consulting with the community for answers, appeasing your angry users and fixing issues. If that doesn't sound appealing, be prepared to pony up a little.

Prices will vary. You'll find one or a combination of the following options:

- Per user billing, with discounts for higher tiers
- Per domain billing, with a maximum number of users
- Appliance-based billing with increased size, feature set and user limits
- Initial fee with subsequent annual maintenance fee(s) — often at a lower amount than the initial fee
- Standard subscription fee: monthly, quarterly, annually
- Monthly cost is typically at 10% of annual cost; you pay for the flexibility of quitting at any time, to the tune of a 20% premium
- Discounts for multi-year contracts
- Premium pricing for premium filtering, typically under the banner of Advanced Threat Protection (ATP) or Targeted Threat Protection (TTP)

For brevity's sake, let's stick with the most common: per user billing. What's a fair price per year? The short answer is the bigger the vendor, the bigger the brand, the bigger the cost to you! Email and network security is a large, competitive market. The biggest brands like Cisco, Intel/McAfee and Symantec can charge anywhere from $40 to $60 annually for email filtering. Their trick? Hiding it in packages with other items.

A fair per user annual price would be $10 to $25 for basic email filtering. For more advanced filtering, you're looking at prices more in the range of $15 to $35 per user, per year. Factors that generally influence price include volume, cloud space and the level of filtering.

QUESTION 6:

ARE FREE EMAIL SECURITY SOLUTIONS TRUSTWORTHY?

What "Location, location, location" is to real estate, "You get what you pay for" is to email security. It's somewhere between a mantra, an absolute truth and a guiding philosophy. Remember it when presented with a free offering. are looking at the system's default settings and many critical security issues that result.

That's not a criticism of free software. The most common free offerings are SpamAssassin for email filtering and Clam AV for anti-virus, both of which function reasonably well and are able to block some threats. For most businesses though, "function reasonably well" is simply not good enough for staff, suppliers and customers.

As with any free solution, you will be expected to a lot of lifting through on-going monitoring and configuration

adjustments. Again, time is money. If you are giving one hour per business day, that's about 255 hours annually. If you charge a modest $20 for an hour for your time, then you now have a budget of $5,000 for your email filtering solution. Oh yes, and every time there's a breach by malicious software (and there will be many), add an additional 5 to 10 hours for clean-up.

QUESTION 7:
CAN I TRUST THE PERFORMANCE NUMBERS COMPANIES PUBLISH?

Unfortunately, not always. When you're seeing numbers like 99.7% to 99.9%, it may means only one in 1,000 malicious emails gets through. Seems too to be true? It might be.

Fortunately, you can often look it up. Some companies will get their software performance measured by independent test groups, with the results being posted freely and publicly. One of the most respected and well-known is Virus Bulletin, which tests both anti-spam and anti-virus software performance.

Here's the thing though: performance numbers from email security vendors are best case scenarios, under lab conditions considered optimal. A close comparison would be fuel consumption numbers automakers publish. Labs are not real life. The auto industry's caveat? The phrase, "Your mileage may vary" (YMMV).

Auto makers hide behind and even drive down fuel consumption numbers. Remember the huge Volkswagen emissions scandal last year where they said their cars were far more efficient than they actually are? Yeah, fortunately there's no evidence of that level of manipulation in the email security industry, but the lesson is you should always be critical of the information provided.

Think of published performance numbers as "potential, optimal performance numbers" for your system. If you tune and tweak your system well frequently, have an email stream that is not out of the ordinary security-wise and work with a vendor that will assist you, you have a good chance of getting close to or achieving those 99% or higher numbers.

That said, no system is perfect and blocks 100% of the bad stuff. Yes, you might see a single test where a vendor actually reached 100%, but it is very rare to see that level in the field. You should be more concerned about the

0.03% or 0.04% that gets through. If it's spam, it's not even a headache to delete. If it's a phish or a virus, and your user falls for it, it's a full-blown migraine.

Some vendors now back their performance numbers with a remediation service. That means if a virus gets through via email and it infects you, the vendor will take all reasonable action to get things back to where they were pre-infection. Most companies charge for these services when they are available, but some include them as insurance.

PRO TIP: BACK IT UP

To stay on top of the situation, you should be doing system back-ups daily and frequently submitting your email security solution to trial testing. Good vendors will offer this option, and don't be too concerned are a little lower than expected straight of the box. Your vendor should also work with you to tweak and adapt the software to your individual security needs. This is a test unto itself: if they don't seem knowledgeable or responsive to issues that arise, you may want to jump ship.

QUESTION 8:

BUT CAN I TRUST THE PERFORMANCE NUMBERS REPORTED BY INDEPENDENT TEST GROUPS?

Yes, but you may want to CSI (Cybersecurity investigate) them first. Namely, look into if it's actually an independent test group and objective. Sometimes test groups are funded by competing companies with a vested interested in the publicized results. (Spoiler: they're trying to make themselves look like the best.)

In email security (anti-spam) and anti-virus, you can trust the performance numbers published by groups like VirusBulletin, AV-Comparatives, AV-Test and ISCA Labs.

Here's are the five key things you need to know about what they do:

- They have elaborate test setups to ensure a fair comparison between the different vendors
- They have complex corpora (sets) of emails representative of the streams a typical business would receive
- Their evolving tests include appropriate portions of legitimate emails, newsletters and malicious or spam emails

- They measure more than just filtering performance — they measure speed of execution of the filtering too
- They put much more emphasis on False Positives (legitimate messages that are caught) than False Negatives (malicious messages that get through)

Being a smart buyer means not blindly trusting these tests or vendors. Remember: vendors willingly submit their offering to these groups. In fact, they pay for the privilege! Once their software has been submitted, they have to live with the publicized results. Vendors prepare for these tests by tuning their system to perform better. Don't think of it as irritating or cheating though. Any good vendor will help you tweak your system, too.

The question to ask yourself is whether you think it is fair to expect a vendor to focus as much on a single customer's performance as they do on an independent test. A good vendor will do so, and you should look for that.

QUESTION 9:
IS A SOFTWARE TOOL ALL I NEED TO PROTECT MY COMPANY'S EMAIL?

Realistically, no. A good email security tool will do most of the heavy lifting for you, but it won't solve all your problems. No tool is perfect and any vendor who claims theirs is is selling you more snake oil than software.

It's an inevitability that some malicious messages will get through any protection tool. Ranging from the annoying (i.e. unwanted newsletters) to the dangerous (phishing, attached viruses, links to compromised sites). The problem is once they have a security tool, users often become complacent. Remind yours that vigilance is key!

Often then most important element of a cybersecurity software is the culture you develop around it. As cited by the CBC, "A recent study by the nonprofit Online Trust Alliance found that of more than 1,000 breaches in the first half of 2014, 90 percent were preventable and more than 1 in 4 were caused by employees, many by accident." Human errors are often a huge threat to security because people are… well, human.

Educating your users to be aware, critical and frequent in their maintenance is essential to any optimized security plan.

Don't know where to start? There are services such as PhishMe, KnowBe4 and OneLogin that will help you run tests on your staff. Fearing becoming the next Sony or Athem, organizations throw money at these companies to send faux phishing and mock malware to their unsuspecting employees. The tests involve sending a series of suspicious emails and then measuring the response. Depending on the results, a course of action will be recommended, often including a cybersecurity education package.

QUESTION 10:
WHY WOULD I NEED AN ARCHIVING SOLUTION?

If you're asking this question, you most likely work in IT and haven't yet gotten that ominous knock on the door from HR, finance or legal. Lucky you. When they do come knocking, you better be ready to answer the question, "Do we have our email information backed up?"

There is a huge amount of information in your company's email — about you, your customers, suppliers, employees, intellectual property, systems, financials… virtually everything important. This necessitates why you would need an archiving solution for your email.

COMPLIANCE

There are thousands of compliance regulations, particularly in the US but also in Europe and the rest of the world. Failing to meet these regulations risks severe penalties. An email constitutes a record of correspondence between organizations and must be produced if asked for.

Here are some of the regulation categories that require compliance:

Sarbanes-Oxley Act (SOX) — For public companies in all industries, mostly US but also outside-US companies with US listings

Gramm-Leach Bliley Act (GLBA) — Mostly for US-based banking, insurance and securities companies

Health Insurance Portability Accountability Act (HIPAA) — For companies that handle information about individuals' medical history

Core to compliance is permanence, or the notion that data must be retained and not altered or deleted. Then comes security, or the requirement that this permanent data must be protected. Finally, auditability is the need for this permanent secured data to be easily accessible to the right people when the time comes. Sometimes, your company will need to retrieve email records quickly for itself. Most often, because you are being sued and need to defend yourself. This is when archiving becomes a component of litigation support A.K.A. the ominous knock from legal.

BETTER MANAGEMENT OF EMAILS

The bigger your company, the more emails you will have and the harder it is to manage all that information. Remember, according the Radicati Group, your users are sending on average 122 business emails per day. A good archiving solution will save space —especially if it is in the cloud! It will also make it simple to restore the emails should disaster strike and streamline efficiency by keeping things organized and easily accessible.

IN CLOSING

Here's the thing: email security is only getting more important? It's a fact. According to the Information Commissioner's Office in the UK, cybersecurity breaches doubled over the last year. Across the pond or not, the trend, unfortunately, is global. You need to have the best tools at your disposal.

Think of it as an investment — for your peace of mind, your company, your users, your suppliers and your customers. Email security is multi-layered. You need the right vendor. You need anti-viruses. You need encryption. You need education for your users. You need to implement everything.

It's a lot to manage on your own. Vircom can help you with all of this. Shoot us an email! We promise our servers are secure.

ABOUT VIRCOM

Vircom, Inc. is a pioneer in email security software, technology, hardware and virtual appliance solutions, and professional services.

AT THE EDGE OF TECHNOLOGY

Vircom was founded in 1994 with a vision to advance technological improvements in network infrastructure through innovative products. This vision evolved as the Internet advanced, and it became clear to Vircom that it too was evolving as a company as it became a pioneer in email security and anti-spam software.

VIRCOM'S STORY SO FAR

In 1994, the Internet as we know it today was not yet to be formed. Vircom started by creating software for digital bulletin boards, the precursors of the Internet, and eventually software for the management and authentication of dial-up and DSL connectivity for service providers.

As email evolved into the killer app of the Internet, we developed one of the first secured mail servers for businesses and service providers. At the same time, we also created one of the first secured email gateways to protect any standards-based mail server. We are proud to say that both innovations (modusGate and modusCloud) were based on our own proprietary and award-winning technology.

Since then, Vircom has evolved into more than a developer of email security software. **We are the IT security partners to thousands of customers representing millions of end users.** We are an IT trend-setting company, always monitoring, analyzing and responding at the edge of the latest threats and attacks.

What makes us different is our proactive approach: by being at the forefront of technological advances, we're one-step-ahead of understanding IT threats and challenges and living up to our motto of preventing future problems before they occur.

Vircom

460 Rue Saint-Catherine West, Suite 600 Montreal, QC, H3B 1A7

www.vircom.com | 514-845-5731