Odds of a Bad Bet

A Wire™ Report

Wire.com
I’ve spent much of the past decade making my living on the international poker circuit. Poker is a game of bluffing and self-control; of strategy and calculated risks.

To be a great player you learn the difference between a good and a bad bet. You learn to master your uncertainty, and see the world in odds and percentages. You train your instincts to catch bluffs because at the poker table, everyone is trying to deceive you. Everyone is probing for weaknesses to exploit, and if you don’t defend against them adequately, they’ll take away your hard-earned chips.

And while poker is just a game, unfortunately many parts of the real world behave like this too. This is especially true for businesses in the digital age; digitisation has provided great opportunity for companies, but also for the criminals who seek to exploit them. In this game of high-stakes cat-and-mouse, it is essential for business owners to build smart, defensive strategies against unscrupulous actors who are determined to win.

When Wire showed me the latest statistics on cyber crime I was astonished at the scale of this problem, especially the enormous risks associated with employees and email. I’m certainly used to taking gambles, but only when they’re smart - either the payoff must be large enough, or the odds small enough, to make the risk worthwhile. But if you’re choosing to gamble via lax cyber-security, it’s literally the opposite way round: the odds are stacked against you, and when you inevitably lose, the costs can be significant and may even lead to the death of your business. By drawing comparisons between everyday risks we are more familiar with (and routinely insure ourselves against), I hope to make it clear just how bad of a bet it is not taking your business’s cyber-security seriously.
Introduction

When running a business, there are always going to be risks involved. That’s the nature of the beast.

Be it an investment risk, a change in strategic direction, launching into a new area, or an acquisition, business leaders take risks every day. Some of these risks might be small, others might be significant enough to change the course of your business and could even be the difference between failure and success. However, these are usually highly calculated risks, and only taken once all outcomes have been considered.

Cyber-security is one of those risks. Businesses are prone to attacks from outsiders; that’s a fact. A cyber-breath can potentially be highly damaging for any business. And the easiest way in? Through your people and their emails. Email is an outdated, insecure mode of communication and collaboration that is still being used in the vast majority of businesses, and it is being targeted by cyber-criminals as the weakest point in your defence. There is a clear need for a shift in how organisations optimise their communications and collaboration so that it is more secure and more efficient. After all, even when you are spotting and managing email threats have you considered the time and investment going into this which could be more productively spent elsewhere?

Business leaders (including CEOs, CISOs, etc.) need to understand that the only way for the odds to be in your favour in this game of risk is if you, as a business, put in the right communication measures to ensure that you are as safe as possible. Be this through alternative collaboration and communication programs to email or raising awareness of these attacks, investing in comprehensive cyber security processes is key. Failure to do so means the house always wins.

This report from Wire, the most secure collaboration platform, was co-authored by international poker star Liv Boeree, and looks at the gambles that businesses are taking with cyber-security because of a lax approach to communication and their ability to respond to it without suffering business damage, losses or violations of data regulation. Liv has used her experience as a high stakes card player to compile exclusive comparisons to everyday risks, hammering home the importance of cyber-security for businesses.

It’s now time for businesses to be the house, not play against the house. Because unless you are a professional like Liv, when you step into the casino, the house will always win...
Generally, businesses are made up of people. Without people, there is no business. As your business grows, your team is also going to grow. For the most part, your employees are the life source of the business. They are the people that are bringing in new business, delivering the goods and making activity run smoothly. However, when it comes to IT security, those same people who make your business run can also be the biggest flaw in keeping it safe.

The figure that “an employee is three times more likely to infect a colleague with a malicious email than they are to spread the flu to their partner,” is a worrying one. The likelihood of an infected person spreading the flu to someone they live with is between 20 and 25%, while 71% of organisations were hit by an email attack in the past twelve months that originated from someone within the organisation spreading a malicious attachment or url to others.¹

This, along with the fact that “your chances of spotting a phishing email are as slim as you hitting a specific number on the roulette wheel” -- when you consider there are 37 possibilities -- is a clear demonstration that there is a real knowledge gap for employees about what a dangerous email looks like. However, there is an inevitability that people will always get duped, no matter what training they receive. Some of the emails that are sent by cyber criminals can be well hidden, posing as amusing or standard emails, asking to be shared around the office. It just takes a casual “forward” and the damage is done. It is a fundamental problem that is akin to gambling - the inherent human flaw in people and their judgement.

Of course, it is not just the employees’ fault. Should it be down to them to understand what form these malicious emails take? Is it not the CEO or other leaders within the business that need to also act with vigilance? But as already mentioned, it is an inevitability that people will fall for such attacks. The answer therefore lies with the implementation of more robust communication solutions, where such occurrences are less likely to take place. It is therefore down to business leaders to make those changes.

40% of staff agree that their organisation’s CEO is the “weak link” in their cyber-security operation. CEOs are, after all, supposed to be leading by example. Therefore, along with all other leaders in the business, the CEO shouldn’t neglect something so important or take that gamble on security. It should be a number one priority, and if it is, not only will your employees be better prepared but you will foster a culture within your business that is cyber-security aware.

A good business leader is similar to that of a good coach in a team sport such as football / soccer. Sometimes you need to concentrate on defence, preventing goals being scored against you. You can’t always go all out on an attack. You have to value both in the same light. In business, you cannot afford to neglect such an important component as cyber-security. So ask yourself. Are you a good coach?

4 in 10 employees believe their CEO undervalues cyber-security.
Of course, whilst all employees within a business -- from the CEO to the intern -- need to be more vigilant when it comes to cyber-security, they are not aided by the fact that these attacks are so relentless. As the research demonstrates, there is a "50/50 chance of your company suffering a costly DoS attack over the next twelve months". Flip a coin. Heads you get attacked. Tails and you don’t. Would you want to bet the security, and therefore the future of your business, on the flip of a coin?

Business leaders cannot fall into the mindset of “it will never happen to us”. The odds are against you, so why would you make that gamble? “Your business avoiding a malware attack (next year) is as unlikely as pulling the Ace of Spades from a shuffled deck on one try”. Breaking this odd down, you can appreciate how this approach needs to change:

— The probability per year of a malware attack on a business was 98% in 2017, so the inverse is 2%²

— The odds of correctly pulling a specific card out of a face-down deck is 1 in 52 = 1.92% ≈ 2%

The combination of people being the weakest link, the inherent vulnerability of emails and the continuous attacks are going to cause any business a lot of problems. You are never going to be 100% safe and the nature of the threats are continuously changing. A secure collaboration tool like Wire, which negates the need for the email, is not going to solve a problem like a DoS attack but it can provide a safer platform for communication and collaboration in the event of an attack so you can keep communicating securely even when primary IT systems are down. There needs to be an effort by business leaders to help their employees as much as possible so that these attacks are less frequent. Not taking that responsibility is too big a risk to take, as the damage can be huge for businesses, whatever the size.

To mitigate this damage, the best bet is prevention.

The chances of your business avoiding a malware attack (next year) are as unlikely as pulling the Ace of Spades from a shuffled deck on one try.

There’s a 50/50 chance of your company suffering a costly Denial of Service (DoS) attack over twelve months.

“Cybercrime continues to plague businesses but it’s a problem that isn’t going anywhere, anytime soon. Emails, in particular, are a huge risk area for business as it’s the main vehicle through which cybercriminals are attacking business.

Businesses can dramatically increase their defences by considering what technical measures they have in place, reducing those risk areas – including email usage – and implementing security awareness training for their employees.”

-- Edward Whittingham, The Defence Works
Can you afford to take the risk?

This report has so far established that cyber attacks are a reality, largely as a result of business leaders taking a bad bet on security. The “weak” points have been identified (people and email) along with how relentless these attacks are.

The stark truth is that when these attacks get through (and they clearly are), the chances of significant damage to the company are simply too high. For comparison, consider your own home. When you buy a house, you naturally buy insurance. Against damage. Against break-ins. Against fire. You are taking a considered gamble with the insurance. What you pay to the insurance company is so small compared to the potential outlay on building or buying a new house. Add this to your mind being at ease that you are covered for the worst is a huge comfort.

A business is over ten times more likely to suffer a week-long downtime from a ransomware attack than you are to suffer a house fire.

Your business was five times more likely to suffer a debilitating ransomware attack in 2018 than you were to be involved in a car accident.
So why aren’t business leaders taking this “safer” gamble? After all, your best bet is prevention and part of that prevention should be secure collaboration. It is one thing to gamble when the stakes are low, but when they are this high (as in the health of your business), can you really afford to take the risk? All of the odds are pointing towards the fact that your business is more likely to suffer from an attack, than you are to “suffer a house fire” or than you “being involved in a car accident.” You wouldn’t take the risk and drive dangerously or without a seatbelt with family, friends and loved ones. You wouldn’t not insure your home? So can you really afford to place the bet of not having secure collaboration tools (compared to the weak link - emails) and afford to live with the ramifications?

Paying to prevent is going to always be far cheaper than paying to fix. That is the smart bet.
The facts speak for themselves. Investment to prevent malicious attacks is a sound one.

It is by far the best bet. And that bet needs to be taken now due to “cyber-security costs [...] rising so fast.” Failure to act now would be the equivalent of “letting ten years’ worth of inflation erode the value of your cash” if you waited for another year to make the investment in more secure collaboration. This is language that all those at the top of companies should understand, and act on.

“Being aware of fraud risk and preventing fraud before it occurs helps minimize the cost to the victim organization, and companies that don’t have protective measures in place stand to lose the most.

When assessing fraud risk, organizations need to recognize that cybersecurity is a pivotal part of their fraud prevention plan.

The current landscape of cyber fraud requires a proactive approach toward preventing it.”

-- Bruce Dorris, Association of Certified Fraud Examiners

The average ROI of cyber-security intelligence investment is twice as high as that of the S&P 500
Cyber-security costs are rising so fast that waiting another year to buy yours [cyber-security] is the same as letting ten years' worth of inflation erode the value of your cash.

It makes business sense, and when you compare the odds of an attack, as outlined in Chapter 1 of this report; “The chances of your business avoiding a malware attack are as unlikely as pulling the ace of spades from a shuffled deck on one try”, “50/50 chance of your company suffering a costly DoS attack over the next twelve months,” and the chances of “spotting a phishing email are as slim as you hitting a specific number on the roulette wheel”, it makes even more sense.

Choose between the sound investment and the odds of attacks. It should be a no brainer.

This especially rings true when you consider that “you’re almost as likely to go out of business due to a cyber-attack as your startup is to fail because it didn’t get the next round of funding”, with 67% of startups experiencing funding failure rate compared to 60% of SMBs folding due to cyber-attack.

While the odds of your startup business failing due to cyber attack are equivalent to failure due to lack of funding, they can be more easily remedied through thoughtful investment in cyber security. The return on investment (ROI) when it comes to cyber-security investment is clear. In fact, it is “twice as high as of the S&P 500” with it being 21.5% compared to the average S&P Index ROI being approximately 10% since its inception. Pay little now, pay even less later.

---


This report shows that people’s use and reliance on email is businesses’ greatest security vulnerability. It is for this reason that business decision makers need to be looking at alternatives. Alternatives that offer more secure modes of communication and greater collaboration within teams.

Wire is one of those alternatives, and was created for that reason. It was designed to address the problem with email but also provide a platform for collaboration that is cost-effective, innovative and ready for the “Future of Work”. Offering high levels of security and privacy by utilising end-to-end encryption, Wire can transform the way businesses communicate and collaborate. The modern workforce is accustomed to a new style of working that is more mobile, more efficient and more instant. This is a workforce that is used to instant messaging and chat-style functionality. This is how they are used to communicating. This is a workforce for which email is increasingly not only a security risk but something that employees hate working with. Wire has recognised this need for an alternative to email, both from a security point of view and to facilitate a better way of collaborating amongst teams.

Now it is time for business leaders to do the same, and join the 700 enterprise customers, including UNICEF, Ernst & Young, BlackRock Ventures and SoftBank Robotics, all of which have adopted Wire since its inception in 2018. Email usage should be something of the past. Wire is THE investment that all businesses need, in order to win the game of risk and reap long term business success.
6 / Conclusion

This report is clear evidence that the benefits of secure collaboration and cyber-security investment in businesses are not being recognised. Despite the clear perils, leaders are still gambling on company security when instead the best bet is prevention.

When you walk into a casino, or sit at any poker table, you know that you have a disadvantage playing against the “house”. As the saying goes, “the house always wins”, and most of the time it does. The best players don’t take risky bets, they keep their cards close to their chests and play the odds. The same applies when it comes to security and privacy. Understand the odds, make the smart bet and you won’t lose as much. Sometimes you might even win!

However, the relentless nature of attacks means that you will never be safe from the modern cyber-criminal and there is no tool, software or process that can completely cover you. The odds in this report may seem to paint a bleak picture, but all hope is not lost. Decision makers within businesses have the opportunity and choice in how they keep these risks to a minimum and moving towards more secure and dynamic communication and collaborative tools. Look at how your workforce is communicating and collaborating, ensure that it is secure and safe and make that company policy.

Wire offers the best of both worlds.

Start a free trial today or contact us for a customized solution.

We can assure you, it won’t be a bad bet...