Reputation and cybersecurity: from risk to opportunity, and cyber-pride

kaspersky

Reputation and cybersecurity: from risk to opportunity, and cyber-pride

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."
(Warren Buffett)

The limits of fear as a motivator – insights from psychology
Fear is useful. According to neuroscientists at the Karolinska Hospital in Stockholm, "The function of fear is to motivate organisms to cope with threats that have jeopardized survival throughout evolution."

But the protective responses of fear (freeze/fight/flight) weren't built to face demons in the modern workplace. Fight has a role to play in the context of an immediate cyber incident, but the fight response can be a blunt instrument, and is always short-term in focus.

Psychologist
Christine Tappolet (Université de Montréal) makes this point succinctly: "Fear influences what we do by narrowing the agent's [i.e. our] focus." We focus only on the threat in front of us right now, at the expense of seeing the wider picture.

In psychology, a distinction is made between Approach Motivation (attraction to something positive – driven by hope), and Avoidance Motivation (moving away from something negative – driven by fear). Both have a role to play but, as psychologist Andrew Elliot (University of Rochester) puts it, "Avoidance motivation is designed to facilitate surviving, whereas approach motivation is designed to facilitate thriving."

In this paper, we invite you to join us in moving from surviving to thriving, by seizing an opportunity to work towards a beautifully positive goal: achieving a powerful and magnetic reputation bolstered by a confident cyber-proud security approach.

Let's start with a very basic and incontrovertible fact: cyber incidents can (and do) damage business reputations. It's very simple: your customers expect you to keep their data safe and their operations running, and if you can't do that, they'll find someone who can. What's more, the risk of reputational damage from cyber incidents is growing.

The value of reputation is nothing new: it's always been one of the most critical assets a business can possess (and the same goes for individuals, come to think of it). Customers don't just buy a solution, service or product; they buy into a brand, an idea, a promise of something greater. Trust is often what clinches the deal.

In the digital age, two key forces have made reputation defense even more urgent than ever before. The first is cybercrime, which opens up companies to attack from remote and unseen malicious actors whose actions can bring a company to its knees. The second is the broader digital context of social media, instant news, and open review sites such as Trustpilot, G2, Feefo and more. Combined, these two forces mean that not only is the battle front larger and more amorphous than ever before, but also that the challenge of containing any negative news (even including rumors) has become relentless, like a game of whack-a-mole.

Join us as we move beyond risk to explore the opportunities of reputation management and cybersecurity

We do need to talk about reputational risk from cyber incidents, and in this paper we will do that, with the cold, hard facts you need to know if you are to commit to defending and protecting your business's precious (and well-earned) reputation for a profitable future.

But we're also going to look at the interplay between cybersecurity and reputation from a completely new angle, one that is very sadly missing from modern discourse on the topic. As well as arming you with battle-critical knowledge on the risks, we're also going to invite you to explore the wealth of opportunity that the reputation challenge represents, in the cybersecurity context and beyond.

We believe that a merely defensive position is woefully unambitious: it fails to do justice to your business, your customers, your mission or your values. Instead, we're proposing an entirely new concept: cyber-pride. Fear has a very valid role to play in forcing us to take necessary actions, but we want to take you far beyond that defensive position and into a world where reputation is treasured, cultivated, celebrated, and no longer jealously guarded like a princess in a tower.

Meet the three reputational pathways

Reputation is not a monolithic construct. It's built up by the cumulative actions of three main pathways, and equally can be destroyed by damage via any of those same pathways. These (in no particular order) are as follows:

1. Product
2. Branding
3. Security

In this paper our main concern is the third reputational pathway – security - but it's worth saying a couple of words about the other two first, because there is significant interplay between the three.

Reputational pathway #1: product

This one looks very simple: your product is good, your customers know it's good, and so they choose you over your competitors. In an ideal world, reputation would depend on product and product alone. After all, wouldn't it be wonderful if all we had to do was build a beautiful product and wait for the sales to come flooding in?

Credit where credit's due: why belief is everything
When your customers buy from you, they credit your account with money in return for products or services. The word 'credit,' comes from the Latin 'credere,' which means to believe. This belief (or lack of it) is what drives purchasing decisions everywhere, from the individual to the largest enterprise. Your customers choose your products because they believe (credit) that you can deliver in a way that your competitors can't. This belief lies behind the financial transaction, which embodies the trust your customers put in you. This trust is earned and strengthened through one of the most phenomenal assets your business can cultivate: reputation.

… and it's not just your customers who give you credit
We shouldn't forget that your customers are not the only group for whom your reputation matters when it comes to credit, belief and reputation. Your business needs access to actual financial credit, and reputational damage can negatively impact your credit rating, making it harder to invest and grow. Insurance premiums can also be negatively impacted by reputational damage, with insurers charging greater sums to businesses whose reputations for cybersecurity are deemed to be weaker.

Reputational pathway #2: branding

A particularly modern pathway, branding has a degree of influence over your business's reputation that is only growing as the world becomes both bigger (by potential market size) and smaller (by the power of the internet) than ever. Branding addresses the fact that customers buy more than just a product, they buy an idea or even a feeling (sometimes tribal) that they aspire to. If your product is good but your branding is poor, you can build, build, build with all your might, but the customers just won't come.

Reputational pathway #3: security

What you'll usually hear about the reputational pathway of security is that lack of it has the power to destroy any of the good achieved by either product or branding in one fell swoop of a cybercriminal's (virtual) axe. We're going to completely overturn that way of looking at cybersecurity in this paper, but we can't avoid the increasingly very sadly true fact that damage to this pathway can and does wreak enormous damage on any of the good work done via the others.

Let's get the negative out of the way as quickly as possible. The reputational pathway of security concerns three key areas, which we've accompanied below with the key questions these raise in your customers' minds:

- Customer data – do you respect me?
- Continual and reliable supply (vs latency) – can I trust you to deliver on time every time?
- Competence – do you even know what you're doing?

Breaking the ice with some cold hard facts

Reputation cannot be an afterthought when it comes to IT security strategies (or any business strategy whatsoever, come to think of it). Reputation is the gold in our Fort Knox, it's the anchor that makes our customers believe in the power of our products and services not only to deliver, but to deliver beyond those of our competitors. The overriding message of reputation is **trust.**

How we know what we know: Kaspersky's International Corporate IT Security Risks Survey

Every year for the past nine years, Kaspersky has conducted a huge international Corporate IT Security Risks survey to uncover exactly what businesses go through when they experience a security incident. The survey covers 23 countries and includes data from almost 5,000 interviews with leaders of businesses across the spectrum. The data from this phenomenal study informs everything we do, guaranteeing that our products and services continue to solve very real problems for a very real world.

The security reputational pathway and the bottom line – facts from our survey

It's very easy to get carried away talking about the value of reputation, and float off into clouds of fluffy marketing talk (not that marketing doesn't have a role to play), but it's the bottom line that counts. That's why our survey pinpoints the exact financial cost of security incidents – we need to know the size of the beast we're dealing with if we are to defeat it.

For the purposes of this paper, we're looking at four categories that attest to the specific financial losses related to reputation that occur in the event of a cyber incident:

1. Lost business
2. Credit rating damage and insurance premium hikes
3. PR costs for damage limitation and reputation repair
4. Compensation costs (the act of saying sorry by way of financial reparation)

Here's how each of these four areas are impacted by the average cyber incident for SMBs and Enterprises:

Category of loss	SMBs 2019	Enterprises 2019
Lost business	$13K	$163K
Credit rating/insurance premiums	$13K	$179K
PR costs	$12K	$161K
Compensation	$5K	$72K
TOTAL reputational loss	$43K	$575K
TOTAL loss per cyber incident	$108K	$1.4m
% of loss due to reputation	40%	41%

The impact of financial losses due to PR-related issues

As well as scoping the scale of financial loss in the event of a cyber incident, we wanted to know the impact these losses had on businesses. We asked our survey respondents whether their organization had experienced any PR-related issues (scandals, public crises) relating to security incidents in general, and data breaches in particular, over the last 12 months, and whether they could estimate how significant the losses were to their company.

Of those who had experienced any kind of security incident, a massive 77% said the PR-related financial losses were either significant or very significant, while for those who experienced a data breach, 80% said the losses were either significant or very significant. Those percentages were the same for SMBs and Enterprises alike.

It's no surprise that insurance companies are starting to offer PR support as part of their service bundles for remediation following cyber incidents. Hiscox (UK) has this included in their coverage:

Public relations costs:
The reasonable costs incurred with our prior written agreement:

1. **for a public relations or crisis management consultant to assist you in re-establishing your business reputation and to respond to media reports, including the development and communication of a strategy to repair your reputation;**
2. **to issue statements via email or your website and social media accounts, including managing and monitoring your social media sites; and**
3. **for any other reasonable and proportionate measures taken to protect or re-establish the reputation of your business.**

What's really shocking about these figures is the fact that a full 40% of all the financial losses a business incurs following a cyber incident comes down to reputational damage alone. For reference, the remaining 60% is lost through the need to employ external professionals, additional internal staff wages, penalties and fines, software and infrastructure improvements, training and hiring new staff.

If we were to isolate reputational damage as a loss indicator, we could naively say that by securing its reputation, a business could reduce loss in the event of a cyber incident by a massive 40%. This approach obviously makes no practical sense (because reputation for solid cybersecurity can only be built on facts, not swagger), but it's a useful way to give reputational damage its rightful place as an area of concern demanding serious, urgent attention.

A holistic approach, rooted in reality and facing the future with confidence

We know that the three reputational pathways are intimately connected, and that none can be addressed in isolation from the others. This is good news – a source of immense power that businesses can leverage to boost their reputation and their bottom line, confident that investment in one pathway breeds returns in the other two. But it does require us to move away from an atomized and negative way of thinking about cybersecurity as a 'mere' defensive tactic, or one that lies only within the remit of IT.

Cybersecurity may be a relatively new issue, but the broader area of **how businesses address risk to their advantage** is older than the hills. In perfecting our approach to cybersecurity, we don't have to reinvent the wheel. To prove our point, we're going to look at another industry that has faced its risk demons head on and come out victorious, resilient and lucrative.

What the car industry has to teach business about cybersecurity and reputation

In 1869, Irish scientist Mary Ward became the first person to ever die in a car crash. Just over 150 years later, car crashes are now the 9th most common cause of death, with 1.2 million people dying worldwide every single year. It's incredible to step back and consider those risks in the context of the estimated 1.4 billion cars on the earth right now, with over 74 million sold every year.

The risks that automobile manufacturers and their customers face are far greater than those that come with cyber incidents: we're talking about nothing short of death and serious injury, which make a data breach pale into insignificance. From that perspective, it ought to astound us that automobile manufacturers now lead their ad and PR campaigns with safety as a key feature. Imagine your own business now, and the risks you're facing when it comes to cyber incidents – would you be willing to lead with safety? Too many businesses prefer to pray that their customers ignore cybersecurity risks when making purchasing decisions, praying too that no incident will occur and, if one does, they'll just figure it out as best they can.

Of course, the car industry wasn't always so bold. For decades during which risks (or deaths, not to put too fine a point on it) increased exponentially, automobile manufacturers preferred to dazzle their customers with the glossy glow of other values and features – glamor, freedom, fun, luxury and engine power. Car companies only took safety to center stage in the 1980s and showcased their proactive defense technologies as an integral part not only of their products, but also of their brand platforms.

Many modern businesses are also trapped in a fear-driven attitude towards cybersecurity and reputational management, echoing the car industry's delay in seeing safety as a prime sale-clincher. This fear, complicated by uncertainty amidst a fast-changing cyber risk landscape, can lead companies to miss unbelievably powerful opportunities for growth.

Take Volvo, for example – widely viewed and independently rated as one of the safest car manufacturers in the world for several decades. And – if you will forgive the pun – this safe reputation was no accident: Volvo was one of the first car companies to understand the positive and profitable relationship between safety and reputation, by leading and differentiating with a bold ad campaign featuring crash-test dummies. The 1987 ad for the Volvo 340 is worth a watch – an elegant 43 seconds that serve as a perfect lesson in why companies must push their safety credentials (cybersecurity chief among them) to center-stage.

Last year, Toyota's New Gig ad campaign followed up on the crash test dummy's role in promoting safety as a core product and brand feature. This time, the crash test dummy is dismayed to find himself out of a job, thanks to Toyota's automated safety features that prevent accidents from happening in the first place.

Volvo's safety claims are based on rock-solid safety technology – and that's why they drive growth

Volvo's reputation for safety didn't sky-rocket on the basis of a simple ad campaign. The campaign only worked because its claims were true, and independent safety ratings have backed them up, time and time again, ever since. In fact, in 2017, the Volvo XC90 was audaciously named 'The Safest Car in the World' by the highest possible independent testers, the Insurance Institute for Highway Safety (IIHS).

Cybersecurity is no different from car safety when it comes to making sure you don't just talk the talk, but walk the walk. This is true from two angles. Firstly, knowing that your business is secure gives you the confidence you need to really promote security as a key value, backed up by action. Secondly, and perhaps more obviously, customers know if their supplier is actually walking (or just talking), either because of a cyber incident that impacts service or leaks data, or because they are becoming more and more adept at sniffing out fakery in corporate values – at calling out baloney and demanding proof of meaningful action.

Before we launch into telling you about how Kaspersky can give you the confidence to promote your business's commitment to security in a way that will drive growth and inspire your customers' confidence, we think it's only fair to present some clear evidence of our own, so that you know we're walking the walk. Making claims about efficacy is easy to do – but unless those claims are backed up by independent testing (like the IIHS and the Volvo XC90), they're meaningless.

We're proud to confidently shout about the fact that we're the world's most tested, most awarded cybersecurity provider, with sustained performance across multiple independent tests that give a far more meaningful assessment than one-off victories alone.

Within that world-leading record of sustained performance lie some key recent accolades that we're particularly proud to lay before you today:

- Kaspersky's Global Transparency Initiative was recently endorsed by the Paris Call for Trust and Security in Cyberspace (see left)
- AV-Comparatives recently congratulated Kaspersky on receiving their Top Rated Product award, as well as other awards for individual tests in 2019
- Kaspersky's Anti Targeted Attack Platform was the only solution to demonstrate 100% detection rate and zero false positives in the Advanced Threat Defense test run by ICSA Labs in Q3 2019
- This year, Kaspersky achieved ISO/IEC 27001:2013 certification; the international standard outlining best practices for information security management systems

These are just some of the credentials that give us the confidence to stand before the 400 million users and 270,000 corporate clients and say **We've got you covered, you're safe.**

We'd like you to share in some of that confidence, so that the voice of your business can rise up above the throng and speak boldly about the respect you place in your customer's data, and in your ability to deliver on time, every time. Sometimes, particularly in the context of the cybersecurity talent crisis, or when budgets and time are under pressure, it can be hard to really embody that confidence – or cyber-pride – in a way that resonates with your customer base.

That's why we engineered Kaspersky Endpoint Security Cloud to deliver exceptional future-ready protection that couldn't be easier to manage. It's bursting with next generation protection technologies, and we're bursting to tell you about them, but first we need to delve deeper into what we see as one of the greatest missed opportunities in business history.

The Paris Call for Trust and Security in Cyberspace was issued in 2018 by President Emmanuel Macron during the Internet Governance Forum held at UNESCO and the Paris Peace Forum. The Call invites all cyberspace actors to work together and encourage States to cooperate with private sector partners, the world of research and civil society, and sets out Kaspersky's Global Transparency Center as a model response to Principle 6 (Lifecycle Security).

"Kaspersky implements a unique approach for higher transparency and verifiable trust in cybersecurity: Kaspersky's Global Transparency Initiative (GTI) puts into effect a set of clear verification and risk-minimization measures to increase users' confidence and ensure that cybersecurity solutions meet and exceed corporate data security and protection standards".

Why don’t businesses lead with their cybersecurity and privacy credentials? Why aren’t they cyber-pride?

According to Forrester, 32% of British online adults, 35% of US and German online adverts, and 38% of French online adults don’t trust any company to keep their personal information safe. We also know that this trust (or lack thereof) is a key factor in purchasing decisions – which come down to credit. With this in mind, it is hard to understand why businesses across the world are missing the opportunity to place their privacy and cybersecurity concerns to the forefront of what they communicate with their customers.

Privacy Notices and the unambitious prison of small-print

There are precious gems confined to the prison of small print accessed by a <Privacy Notice> link nestled quietly at the bottom of web pages of companies of all stripes. These gems should be mined, polished and put on display.

The average company Privacy Notice features a short descriptive opening statement that speaks to customers’ very valid concerns about the use of personal information, but descends immediately into a rambling torrent of legalese: unappealing, and interspersed with only the very occasional explicit assurance of the value that the company places in its customers’ data and security.

We’re not suggesting that every single web page or piece of marketing collateral should lead with statements about cybersecurity and data confidentiality, but rather that these need to move beyond the shadowy prison of small print. Cybersecurity and data confidentiality must be integrated across the business in a holistic way, one that recognizes the primacy of such concerns as an opportunity for driving business growth, rather than as an unambitious pandering to regulatory requirements.

Regulation should not be the sole guide of cybersecurity and privacy policies

Many companies buy into the illusion that regulations are sufficient as a guide to cybersecurity and privacy decision-making. This again speaks to decisions driven by fear and the quest for indemnity, rather than the pursuit of ethical excellence and business growth.

Firstly, regulations struggle to keep up with the pace of technological advancement, either on the business side, or on the side of cybercriminals and their ever-changing methods of wreaking malicious havoc. While regulations must clearly be met, true business leaders will always look beyond current stipulations, guided by the reality of technological innovations on the one hand, and the unchanging eternal ethical principles that (ought to) drive the regulations in the first place.

The good news here is if businesses accept and advocate for the centering of ethics in cybersecurity and privacy, as analysts such as Forrester have done, they naturally find themselves with a powerful opportunity to promote the ethical value of their brand in a way that is backed up by solid action. This is a concrete example of the interplay between the reputational pathways of branding and security.

After all, it’s one thing to say ‘We treat your data with the utmost respect, and here’s how we fulfil all the relevant regulations,’ and quite another to step back and build an ethical and holistic approach to cybersecurity and privacy into a key feature of your product and your brand. When cybersecurity and privacy decisions are driven by deeply held ethical values and not by regulations, a company’s public messaging on respect leaves the tokenistic kowtowing to regulations behind and instead rings true in the perceptions of customers and prospects.

In short, if you want to leverage cybersecurity and privacy to drive business growth, you don’t say that you care – you show it, boldly, and at every single (relevant) opportunity. It’s the air that you breathe, it’s the products that you build, it’s the culture of your organization as a whole, and everyone has a part to play. The organization that achieves this eminently achievable goal (as Volvo did with car safety) secures a powerful and enduring differentiating factor from the rest of the crowd, who remain crippled by their hyper-focus on regulation at the expense of positive ethical action.

Seize the great missed opportunity today and use your reputation to drive growth, with Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud eliminates risks, giving your business the confidence to leverage cybersecurity to drive growth, towards a secure, profitable, and exciting future. As well as knowing your business is defended by the world's **most tested, most awarded cybersecurity provider**, you'll be able to share that confidence in everything you communicate with your customers and stakeholders. That confidence results a clear differentiator from competitors who lag behind in leveraging the reputational pathway of security, like automobile manufacturers before Volvo's bold and lucrative move in the 1980s.

Kaspersky Endpoint Security Cloud is tailor made for the era of cloud, remote working and BYOD – a real-world solution that's easy to use, and puts powerful protection and controls into the hands of businesses whose targets are set decisively on growth.

One of the technologies you'll get that we're particularly excited about is NEW Cloud Discovery, which automatically prevents your employees from indulging in unauthorized cloud service use. It completely removes the stress that can come with having to micromanage the mushrooming array of cloud services that could potentially threaten your business's security.

You'll also get Kaspersky Security for Microsoft Office 365 as part of the package: our dedicated defense solution for the entire Office suite is particularly essential given that Microsoft products are still the number one target for cybercriminals.
Now that remote working is becoming increasingly common, we've added two free mobile licenses per user, so you'll get a solid umbrella cyber defense that recognizes you employ people and not devices. You can even enforce security policies remotely, so your employees will be protected wherever they work – whether in a café or on the beach.

Kaspersky Endpoint Security Cloud is hosted in the cloud, so you don't need hardware or software, or pay for provisioning and maintenance. You'll get instant protection with predefined security policies developed by our professionals, and it comes on a monthly subscription to free up financial resources.

To our 4,000 international experts, **security really is everything.** We live, breathe and love cybersecurity so that businesses all over the world can take our passion and the accolades that come with it to build a solid base for advancing, exploring and discovering the future.

Talk to us about how you can become cyber-proud and build a secure reputation to drive growth with **Kaspersky Endpoint Security Cloud**.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky

BRING ON
THE FUTURE