IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Is There a Special Place for Cybersecurity Marketing?

Andy Harris

Andy Harris
Chief Technology Officer
Osirium

Biography

Andy Harris is the Chief Technology Officer at Osirium (https://www.osirium.com). In a long and distinguished career, including being Technical Director at Integralis, Andy has invented many leading-edge technologies including IP Network Translation Gateway, Print Symbiont Technologies for LANbased printers and Disaster Master, a technique of continuously updating a backup site with mirrored data.

As one of the Co-Founders and CTO of MIMEsweeper, Andy was the creator of the world's first content security solution which became the default product in its space. Andy went on to start WebBrick Systems which was one of the pioneering Home Automation technologies, also a forerunner to what we know as IOT devices today. As Engineering Director, Andy has created and patented several core components in the Osirium product family.

Andy blogs at https://www.osirium.com/resources/blog

Keywords Cybersecurity, Branding, Marketing, Budgeting, Messaging, Cyber threat, Ransomware
Paper type Research

Abstract

The cybersecurity market is now estimated to be around $200 billion mark, but with such a wide choice of cybersecurity products and services on the market, and with the industry constantly pushing the message 'Your business – safe at the speed of light', many businesses are feeling overwhelmed. In this article, the author looks at what's really going on behind the marketing spin.

Introduction

Banks and Perfume are two markets which have the most abstract and often bizarre marketing campaigns – and it often seems like Cybersecurity is not far behind – "Next-gen AI driven peace of mind at the speed of light". Worldwide, the perfume market is £40 billion, the UK market is £1.6 billion alone. In 2020 the worldwide Cybersecurity market was estimated at $139.77 billion, with 2022 estimates hovering around $200 billion.

What's being sold:

Perfume: Personal freshness (Personal 'Brand')
Banks: A notion that they might help one day
Cybersecurity: Nothing happens – business as usual.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Of course, it is more complex, there's a lot of personal choice in perfume and banks have a wide range of products that deal with money. If we think about the transport market, we are never sold 'generic transport', if we see a marketing piece we quickly know if we're being offered a car, bus, ship, plane, tractor, lorry etc. Even within this we can determine what's on offer, from a rib to a cruise ship and for cars we certainly know what the target markets are. Disk drives are the polar opposite sold almost entirely on specifications – size, speed, IOPs longevity. Cybersecurity just doesn't have readily understood metrics.

Cybersecurity has a wide range of products, but here's the market difference, customers are told that different products solve the same issues. There's no real differentiation – we all bombarded with the same messages.

Why? Well, obviously the $200 billion market has a lot to do with it. It means that US based venture capitalists can fund multiple companies at massive levels since the returns across several investments will be worth it. It's not unusual to see US startups initial funding at $50-100 million[1]. European startups are funded at roughly 1/20th at 1-3.5 million euros[2].


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

There's a key difference in operation, for a US funded start-up they will work on the product and the marketing at the same time - in order to make an early impact. European companies will use the funding to create the product and then seek further funding when they have a proven product running at paying customer sites (typically 1-5 customers). Therefore, it often appears that European companies have been around for longer.

There's a huge difference in marketing budgets, many US companies will be spending at least 60% of their year budgets on marketing, right from start-up. The Europeans will start at 0% and work up to around 20%. This helps to explain both messaging and company survival.

Larger companies will message at the top level of big organizations in their local market. Whereas smaller cybersecurity startups will target the people with the need for instance, the senior operational people in cybersecurity teams.

Why do smaller cybersecurity companies survive?

The main factors are:

- **Problem based engineering** – the developer to customer chain is short, the devs will have often met with the customer to get that one-on-one understanding. This hones the product features into those that are needed rather than what an industry analyst thinks are needed. That low marketing spend means more available resource goes into the product.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

- **Engineers as Marketers** – the early days of light funded cyber-startups will often see tech staff stepping up to the marketing plate. They think different, and a clumsy but accurate description of a solution to a prospects problem trumps the feel good 'business at the speed of light' message. For the venture capital funded companies the marketing budget is so high that it will be subject to venture capital oversight – which means that the venture capitals need to understand the messages as well.

- **Vertical care** – everyone in a light funded company cares about customers – so it doesn't matter how the customer approaches they'll get a warm welcome.

- **Salaries** – Salaries outside of the US salaries are considerably lower.

Message abstraction

Marketing naturally seeks to extract the simplest messages about their products. Perhaps we are too obsessed with the 'Elevator Pitch'. This is where the messages like: "Your business – safe, at the speed of light" comes from. The reality is that cybersecurity is complex, as an industry we rarely acknowledge this. The industry will gleefully tell you how complex an attack is, but never tell you the full story about lasting solutions.

Often the size of a company affects how close the messaging people are to the product. The bigger, the further away and therefore the more abstract it becomes. It's worth noting that this again is a cybersecurity effect. Consider Cisco, look at their switch marketing compared to their cybersecurity marketing. Let's be clear Cisco has excellent marketing and a great reputation for acquiring other businesses carefully.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Funding tends to drive the message, heavy funding – feeling based messaging, light funding solution-based messaging. This line is blurred, because the marketing departments of growing companies will emulate their big budget competitors.

Different products same threat

This is one of the more perplexing aspects of cybersecurity – why does it seem that all the products address all the threats? A few years back this would have been driven by flavour of the week, but these days it's pretty clear that ransomware is by far the biggest threat.

It's driven by crypto currency which has given our adversaries the opportunity to anonymously monetize their actions. If we cast our minds back to 1989 and the first ever ransomware authored by Joseph L Popp we'll remember that he used a PO Box in Panama for ransom collections. He was easily traced by Scotland Yard and arrested by the Dutch at Schiphol airport. We can contrast this with Bitcoin where it is almost impossible to trace transactions. Even when wallets are associated with individuals it's most likely in regimes that enjoy the circulation of hard currency, particularly if it flows from the West. Joseph went on to found a butterfly conservancy[3].

Money has driven the shift from single coders to multi-discipline teams creating ransomware. This means that modern variants have many moving parts:

- **Mutator** – Continuously change the layout of the code fragments to avoid signature detection.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

- **Dropper** – A small code fragment that when executed pulls together elements of the attack from many places.

- **Replicator** – Code that moves the attack laterally across an organization, generally working on file-shares and the like.

- **Listener** – Keylogger functionality that listens for login activity to harvest credentials for use in ex filtration, bricking and wiping.

- **Ex filtrator** – Code that selects, fragments and temporarily encrypts data to be send back to the attackers.

- **Command Shell** – Code that sends and receives commands. Typically, it will listen to social media or other common locations for commands. It can use previously stored credentials to connect to other architectures (for example, hypervisors). Once connected to those systems, commands can be issued to delete backups/con figurations, encrypt data (such as virtual machine images) or destroy firmware.

Then there are the actual payloads, which at the time of writing are:

- **Encrypt** – Encrypt the victim's data in place, ransom for the keys to restore.

- **Ex filtrate** – Copy victim's data, ransom to prevent publication.

- **Brick** – Render victim's hardware devices useless, by destroying sections of bootloaders or in the case of secure boot devices corrupting key stores. Devices become uneconomic to repair.

- **Wipe** – Render victim's disk-based data useless and beyond the reach of data recovery organizations. Typically achieved by destroying partition tables, file allocation tables, file headers and the master boot record. This is actually a very small amount of data compared to the overall size of any disk.

So there are ten moving parts of ransomware. We can deduce that different cybersecurity products will target these parts with a variety of strategies.

A view of the market

You may find it useful to consider that cybersecurity products fall into these categories:

- **User Behaviour** – is focused on educating the users not to click on what could be a dropper or replicator in the first place. It could be education, or an extra step in the way of opening email attachments.

- **Monitoring** – addresses everything that is moving in your organization. It does not stop anything on its own but does tell you when something changes.

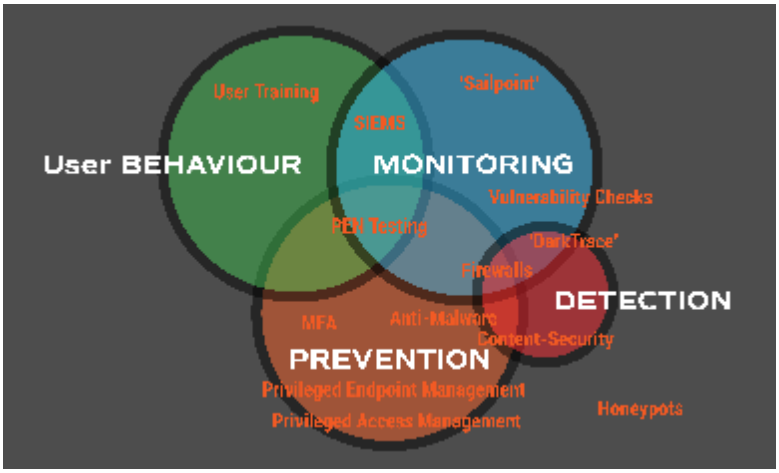
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

- **Detection** – finds the presence of threat in your organization, typically by code signatures, behaviours or alerting you to known vulnerabilities.

- **Prevention** – seeks to stop any action the threat has. This can be through removing privileges, separation of threat code and systems, or separation of users and credentials. Multi-factor Authentication helps to render stolen credentials useless to attackers by requiring an extra step.

Figure 1: Cybersecurity product classes



Source: Osirium

There are combinations of these classes, for example a monitoring product could issue rules to prevention and detection products based on unusual activity. To take us back to marketing, monitoring products have the most abstract messaging. This is because they are all about information and it is the customers that have to take action. In development terms they are great products – the business does not stop if they fail. They tell you so much all the time that if you do get caught it was your fault for not taking notice.

You could have a wry smile that cybersecurity monitoring products are most likely to sponsor Formula One teams. When combined with prevention, monitoring products can become fragile. This is because the AI elements are often dealing with unconstrained problem spaces. The marketing messages tell you that these products work out what is normal for your organization and then jump on anything that is a change (because change is bad right?)

Real organizations are under continuous change, none more so that IT teams, who as soon as they have delivered one project are on to the next. Occasionally jumping back to previous projects as operational issues arise. All monitoring products will tell you that your IT department is the greatest risk (so actually they are right! But remember that data is not information).

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The value of AI in monitoring is noise reduction. Whilst we've just had a jab at monitoring, a decent SIEM system is essential – so long as you remember that every pound you spend is wasted if you don't look at the reports.

The failure anomaly

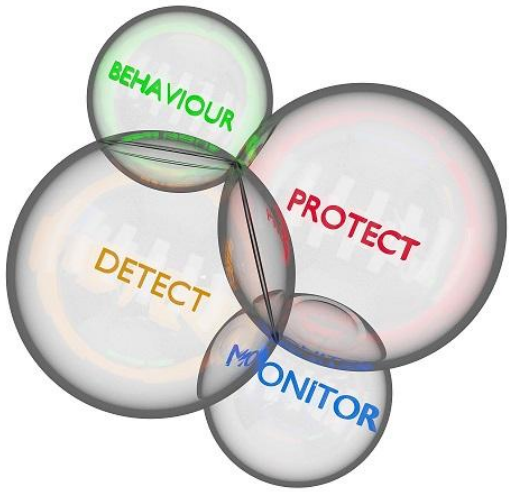
It's curious that the cybersecurity industry never talks about failure. We can compare this with, say, Cisco switches which are known for their cost, function and reliability. Still given all that. Cisco publishes many documents and has numerous training courses on how to create a resilient network.

Ask at a trade show and you'll get the answer – "we've never known it fail" along with "well you buy an extra box if you're worried". The cybersecurity industry will follow the same patterns of software failures as any other market segment. There are some key differences, for example secure programming practices. One could argue these lead to more reliable products but in reality it leads to more complex failure modes (more lines of code statistically more errors). The most common failure of cybersecurity products is configuration. Where a configuration allows too much through, or blocks a critical function.

Real security

Seasoned SysAdmins know that you need products in each of the categories to be secure. You can't trust the users, they will choose weak passwords, share stuff where it shouldn't be shared, and occasionally click on the bad stuff. They need education and care; you can phrase training in terms of how they would protect their own social media and banking.

Figure 2: Elements for real security



Source: Osirium

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

You need to monitor all the things all the time – and take note of the reports. You need to detect every known vulnerability as soon as possible – there is no lag in your adversaries take up. They will be coding against new vulnerabilities within minutes of announcement. (This could lead us down the route of Common Vulnerabilities and Exposures (CVE)s – a list of publicly disclosed vulnerabilities and exposures – and why these are right for the reputation of the whole cyber security industry).

Prevention is key. Users can't be trusted with local admins rights or unfettered privileged access to systems. To conclude, perhaps you'll think about where the money goes in the cybersecurity world. We hope we've given you an insight into decoding the marketing messages.

Reference

1 Wiggers, K. (20 July 2022), Crunchbase looks to grow its database of startups with $50m in new cash. Techcrunch. Available at: https://techcrunch.com/2022/07/20/crunchbase-looks-to-grow-its-database-of-startups-with-50m-in-new-cash

2 https://www.eu-startups.com/category/fundin/

3 https://www.tripadvisor.com/Attraction_Review-g48333-d1755655-Reviews-Joseph_L_Popp_Jr_Butterfly_Conservatory-Oneonta_New_York.html