AT&T Cybersecurity

AT&T Business

Confidence: The perception and reality of cybersecurity threats

A breakdown by industry and company size

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning—helping enable our customers around the globe to anticipate and act on threats to protect their business.

Table of Contents

1. Executive summary

1.1 Introduction

Another RSA conference has come and gone. It is arguably one of the largest business-focused security conferences in the world. It attracts security professionals and companies from around the world, and it's where many security vendors launch their companies, new offerings, or other major announcements. This makes it the perfect place to take the pulse of the industry at large.

We once again took the opportunity to run a survey at our booth. And this year, due to the recent acquisition of AlienVault® by AT&T to form AT&T Cybersecurity, we launched the new division at RSA. It therefore meant we had two booths covering both the South and North halls. This allowed us to find out not only what the sentiment is around the industry as a whole, but also how this sentiment potentially differs based on the size of the company, or the industry sector in which it operates.

1.2 Methodology

This report is based on a survey of 733 participants at RSA 2019 and interviews with security experts. Additional threat data specific to industry sectors was provided by AT&T Alien Labs™.

In a change from previous reports, we also captured the demographics of the survey participants to identify where findings represent the general industry or where particular findings are more relevant to the size of a company or its industry sector. These questions were optional, which is why the total count in each chart has some slight variance. However, even with this variance, we believe the sample size is statistically significant and the variance introduced by opt-outs does not materially impact the overall results. The total demographic breakdown is in the table below.

Sector	5,000 employees or less	5,000+ employees	Totals
	490	**243**	**733**
Financial services	73	35	108
Healthcare	32	22	54
Hospitality	5	8	13
Manufacturing	36	21	57
Other	218	92	310
Public sector	52	18	70
Retail	27	16	43
Transportation	6	8	14
(blank)	41	23	64

In terms of company size, there isn't a universally agreed upon definition of when an enterprise is considered small, medium, or large, so for the sake of this report, we are considering companies with up to 5,000 employees as being in the SMB space, while companies with over 5,000 employees are large enterprises.

This report was written by Javvad Malik, Security Advocate at AT&T Cybersecurity.

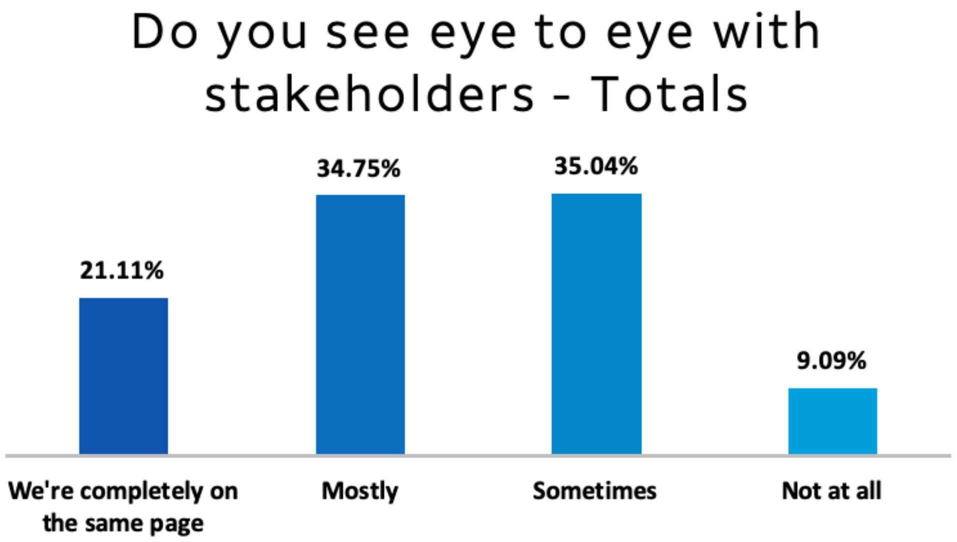
1.3 Key findings

- Large enterprises are more aligned with stakeholders. Of the industries, retail was the most negative in terms of seeing eye to eye with stakeholders, with 17% of participants stating 'not at all' and a huge 43% stating that they only saw eye to eye with stakeholders "sometimes."
- The biggest threats that worry companies of all sizes are phishing (29%) and cloud security threats (27%).
- Only 17% of smaller enterprises are very confident in defending against DDoS attacks compared to 29% of large enterprises. Additionally, only 15% of smaller enterprises are very confident in defending against IoT attacks compared to 21% of large enterprises.
- The majority of companies view supply chain security as an essential component of any security function (37%), although 18% of smaller companies feel these activities take away resources from important work, and 19% believe it merely serves as a "tick box" activity.

2. Seeing eye to eye

For many years, the security industry spoke of the need to have a voice at the highest level in the organization. With so many breaches over the years, there are few executive boards, if any, that aren't in some way concerned about cybersecurity.

But what we wanted to know was whether or not security professionals feel like they see eye to eye with executives.



Overall, the results weren't too surprising, following a standard bell curve. With only 9% of participants answering "not at all." As one would expect, the majority of responses fell in the middle of the spectrum.

2.1 Eye to eye by size

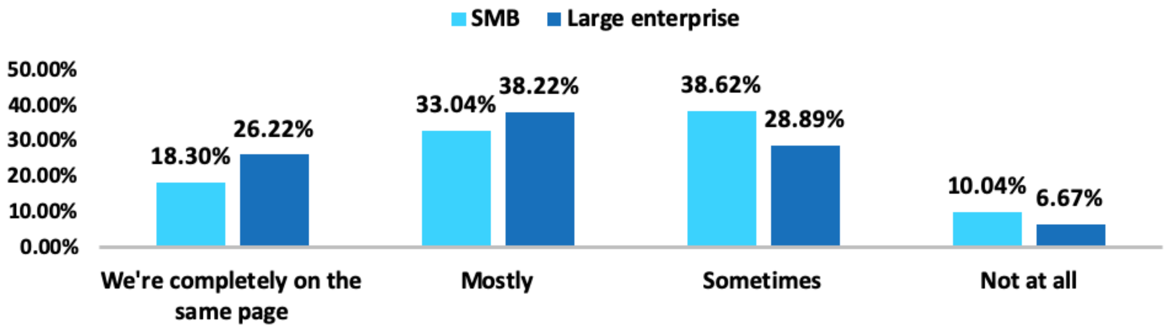
When splitting the results out by company size, a slightly different picture emerges. While the bell curve remains consistent, we see that larger enterprises appear to have a far better alignment with their stakeholders than small or medium businesses (SMBs).

Only 18% of SMBs state they were completely on the same page with their stakeholders. By comparison, 26% of large enterprises said they were completely on the same page.

On the other side of the spectrum 10% of SMBs felt they were not at all in alignment with their stakeholders compared to just under 7% of large enterprises.

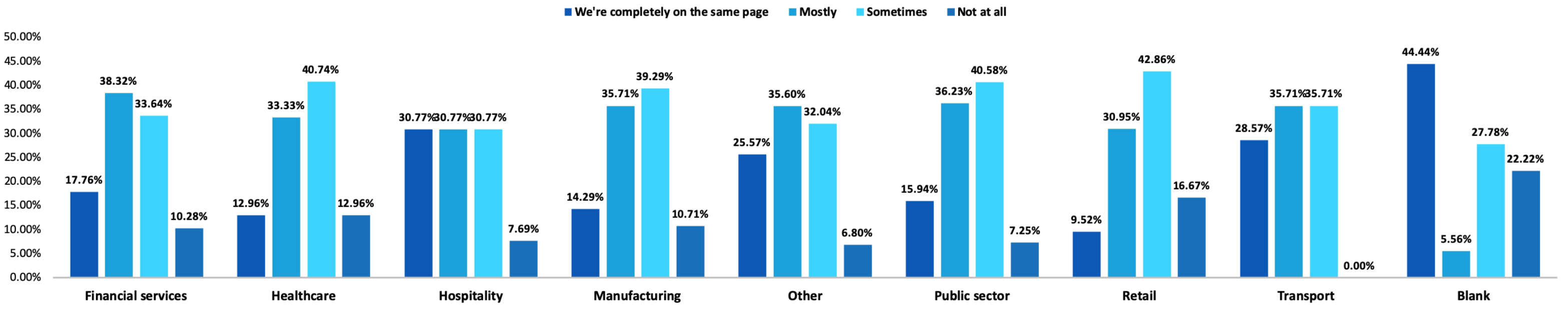
This outcome is not all that unexpected; large enterprises usually have robust security governance in place, and many issues are discussed from a business risk perspective, allowing there to be better understanding. By contrast, smaller companies may have fewer stakeholders which have less time to dedicate to governance, especially when hitting targets is a priority.

Do you see eye to eye with stakeholders by company size



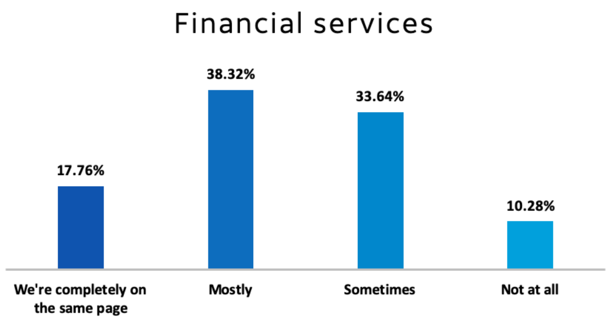
2.2 Eye to eye by industry sector

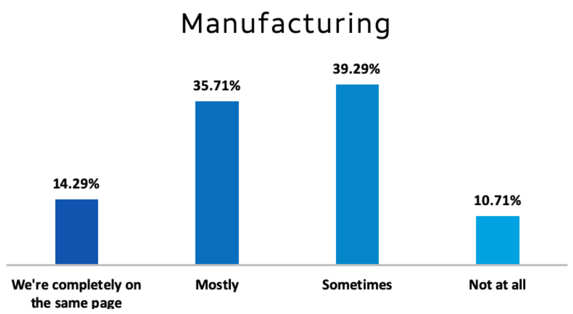
Do you see eye to eye with stakeholders by industry vertical

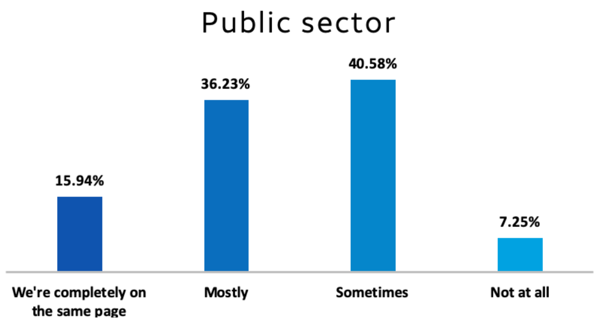


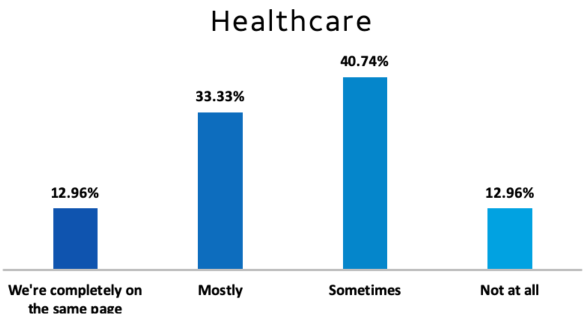
Looking at the results through the lens of industry sector is worthy of further discussion.

Financial services, manufacturing, and the public sector had a rather typical distribution curve that matched the aggregate distribution.





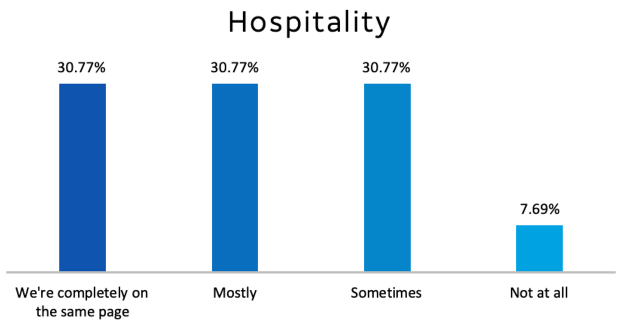


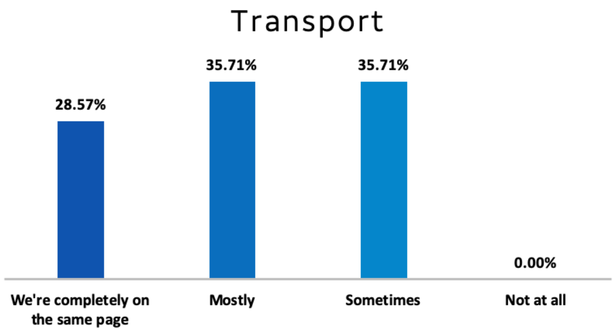


Healthcare, also followed a similar curve, although it was more negative overall with more participants inclined to believe they only saw eye to eye with execs sometimes, or not at all.

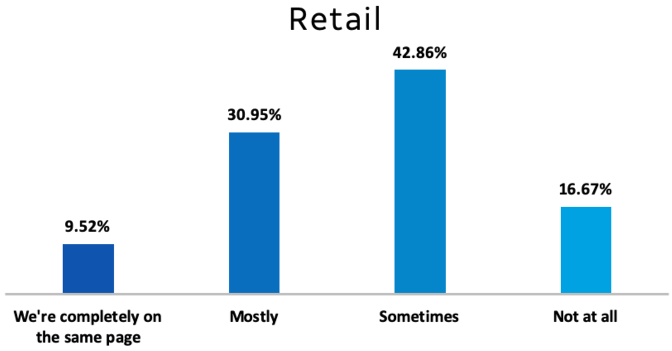
Hospitality was overall optimistic, having an almost even split between being completely on the same page, mostly, and sometimes. Only 8% stated “not at all.”

Transport was even more positive than hospitality, with no participants stating “not at all.”

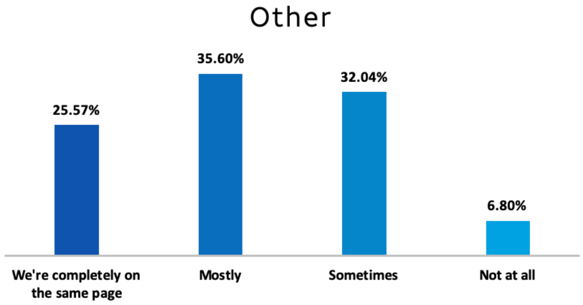


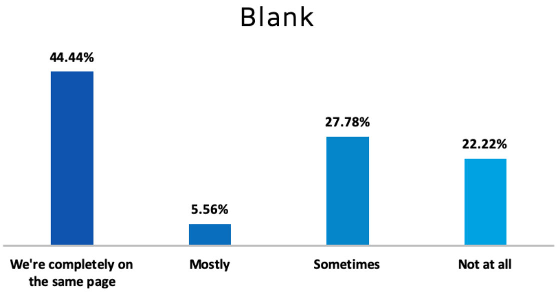


Retail was the most negative of all the sectors, with 17% of participants stating “not at all” and a huge 43% stating that they only saw eye to eye with stakeholders “sometimes.”



Participants that identified as working in other sectors were more positive than the named ones. While those that opted to not disclose their sector (blank) had a skewed result which didn’t follow the usual trend: 44% stated they are completely on the same page, and only 6% said they were “mostly” on the same page.





3. Threats

The threats companies face vary and change rapidly, but there are some visible trends or common techniques attackers use, whether it’s taking advantage of internal weakness, user error, or external tools and methods.

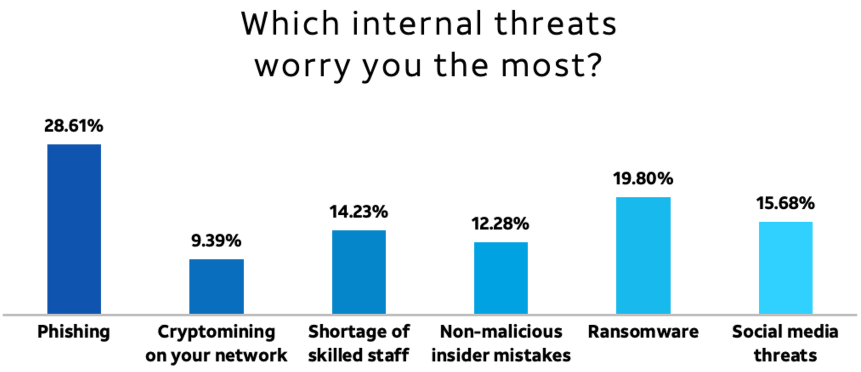
We asked two sets of questions to get a better understanding as to which threats are most concerning for companies. These questions broadly split the threats into two categories: internal and external threats.

3.1 Internal threats

At 29%, nearly a third cited phishing as the threat that worries them the most.

Phishing comes in different guises for different purposes. Sometimes phishing emails are used to deliver a malicious payload. Other times it’s to social engineer the recipient by gaining their trust or scaring them by posing as an authority to get them to make payments—as we often see in business email compromise (BEC) attacks.

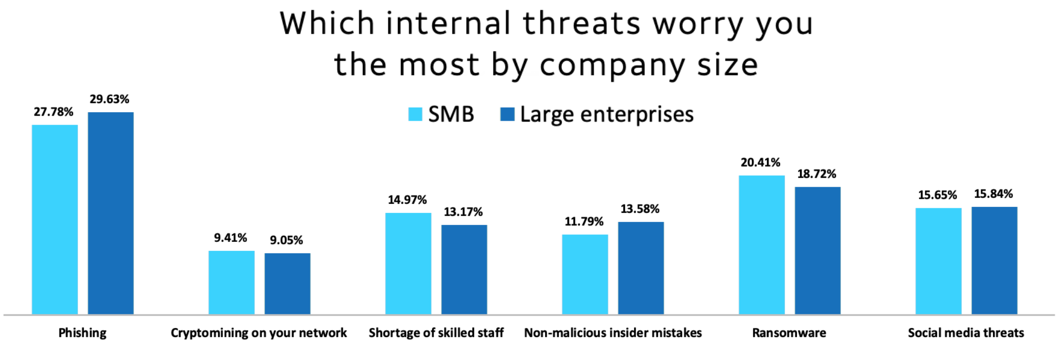
Ultimately, this likely boils down to the fact that for most cyber threats, a technology solution is usually available to ward off attacks, but with phishing, most systems rely heavily on the email recipient being able to detect and respond appropriately.



In second place comes ransomware, which has entered into the vocabulary of nearly everyone in the last few years. The biggest challenge with ransomware is that, unlike other attacks, there is no hiding from the fact that systems have been compromised; and even if recovery is quick and without any loss of data, the reputational damage can be detrimental.

Social media threats showed up in third place, with 16% of participants citing it as a worry. This, perhaps surprisingly, is ahead of having a shortage of skilled staff. Delving into this, though, it makes perfect sense. Social media has rapidly become an unmanaged and uncharted source of risk for many companies. Any mistake can impact brand and trust, expose sensitive information, or indeed become a source of entry into an organization.

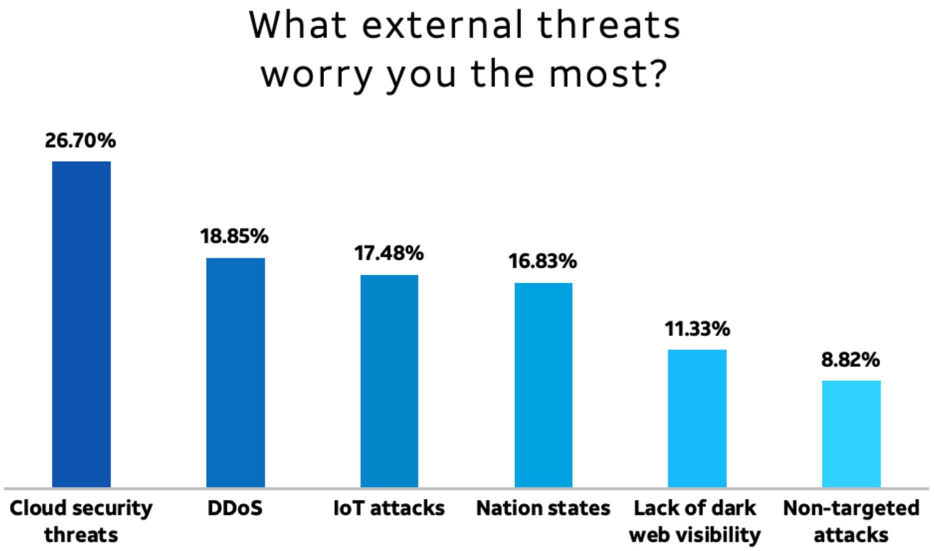
The internal threats remained almost identical across companies of all sizes with no change in priority or any great variance in responses.



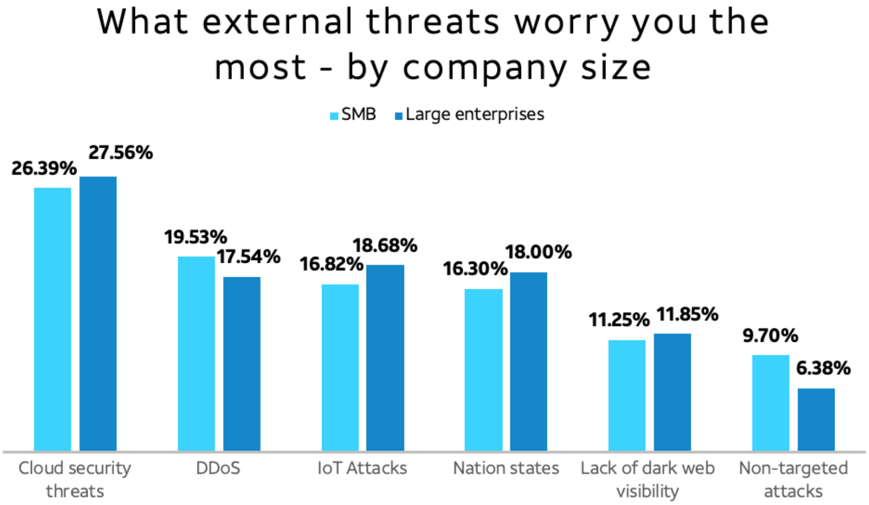
3.2 External threats

When asked the same question about external threats, cloud security threats were cited as the most worrying in 27% of all responses. While it may feel as if discussions around cloud and cloud security have been ongoing for many years, it is still a relatively new area for many companies. The implications of moving to the cloud with or without a well-defined strategy are being felt today, and with so many data leaks attributed to misconfigured cloud databases, or through poor credential management, companies are right to be worried.

Distributed denial of service (DDoS) attacks were in second place, closely followed by Internet of Things (IoT) attacks and nation states.



Much like internal threats, there wasn't a great deal of difference in the results based on company size. The small differences in responses were to be expected. SMBs were slightly less concerned with cloud threats, IoT attacks, nation states, or visibility into the dark web and more worried about DDoS and non-targeted attacks.

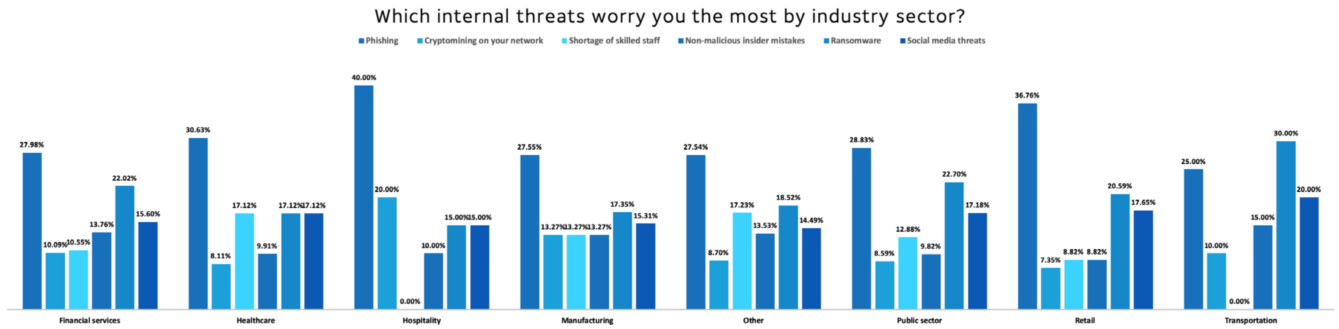


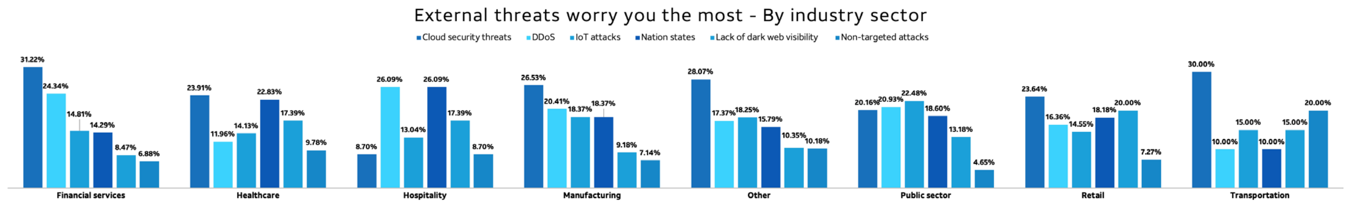
3.3 Threats by industry sector

One of the more interesting views we got from this survey is how different sectors view threats. We compared them to the threats AT&T Alien Labs saw across different sectors.

Even a cursory examination at how sectors rated threats provides some interesting insights. For example, the hospitality sector has the lowest rating of cloud security threats compared to any other sector, at just 9%.

The retail sector places the greatest emphasis on dark web visibility compared to others, and the transport sector is the most concerned with non-targeted attacks.


Which internal threats worry you the most by industry sector?


External threats worry you the most - By industry sector

Neither the hospitality nor transport sectors were concerned about the skills shortage, but transport was the most concerned about social media threats and ransomware at 20% and 30% respectively.

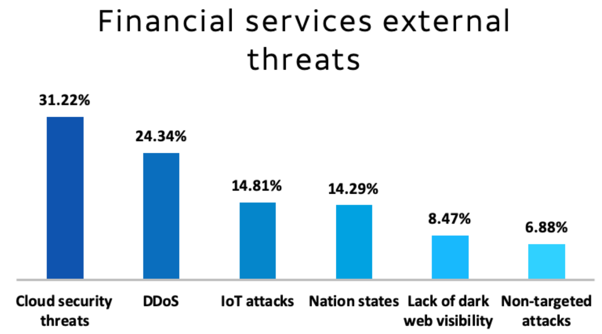
Let's take a deeper dive into each industry sector with what AT&T Alien Labs has been observing.

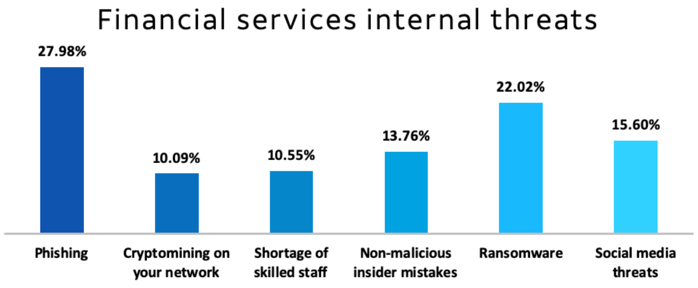
3.3.1 Financial services

Financial services face a diverse set of cyber threats, with many targeted threats falling into the category of criminal gain. There is a wide range of attackers targeting both banks directly and their customers.

Targeted threats

The two main categories of targeted threats against financial services fall under the category of criminal gain and sabotage, which have a number of active groups and nations. Based on this, it is surprising to see that of survey respondents who worked in financial services only 14% stated nation states were a worry.





North Korea is a significant threat, with reports the government has attempted to steal billions in aggressive attacks against both state and private banks.

In a particularly brazen attack, they attempted to steal almost $1 billion dollars from the Bangladesh state bank, though only got away with $81 million dollars.

Some reports relating to North Korea include:

- Lazarus Resurfaces, Targets Global Banks and Bitcoin Users
- A New Version of North Korean Ransomware Hermes Has Emerged
- High alert against malicious code attacks in Vietnam
- Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant
- APT38 Unusual Suspects
- Lazarus Under The Hood

Other groups include the now defunct FIN4, which used to target financial institutes for trading information.

FIN7 and Carbanak are infamous groups of attackers that have successfully stolen millions of dollars from banks.

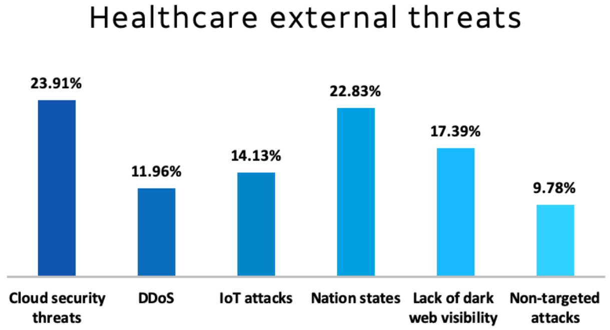
Other groups active in the financial services space include Dridex, Cobalt Gang, and Emotet, among others.

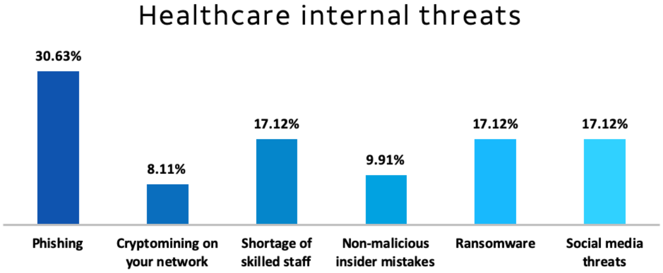
Russia has been involved in a number of attempts to disrupt the financial sector in Ukraine by attackers who have also successfully disrupted the power grid.

3.3.2 Healthcare

Only 17% of the healthcare industry cite ransomware as a concern. This is somewhat surprising considering during 2018, a number of organized criminals moved to targeting healthcare providers with ransomware due to the criticality of continued operation.

The group operating SamSam ransomware is thought to have earned over $5 million dollars manually compromising critical networks and deploying ransomware. Healthcare is a key target.





Defending against SamSam is more akin to a targeted attack than typical opportunistic ransomware. SamSam attackers are known to:

- Gain remote access through traditional attacks, such as JBoss exploits
- Deploy web-shells
- Connect to RDP over HTTP tunnels such as ReGeorg
- Run batch scripts to deploy the ransomware over machines

A more detailed analysis of these attacks is available in the AT&T Alien Labs blog "SamSam Ransomware Targeted Attacks Continue" and the following reports on OTX:

- SamSam Ransomware Campaigns
- SamSam - The Evolution Continues Netting Over $325,000 in 4 Weeks
- SamSa Ransomware
- SamSam: The Doctor Will See You, After He Pays The Ransom

Other ransomware observed targeting health care includes:

- Defray Ransomware
- Off-the-shelf Ransomware Used to Target the Healthcare Sector
- Detailed recommendations for preparing for SamSam and related destructive attacks is provided by HHS, FBI, and US-CERT.

3.3.3 Hospitality

Hospitality faces targeted threats from groups seeking criminal gain and espionage. It is therefore an accurate reflection of this that nation states and DDoS are joint primary concerns for external threats, and phishing is by far the biggest internal threat—especially given spear phishing is a favored tactic by attacker groups.

FIN7 is thought to have stolen over one billion dollars from companies, and over 15 million credit card numbers. Restaurants were a common target, and FIN7 was known to send spear-phishes claiming someone had food poisoning to entice the victim to open the malicious email.

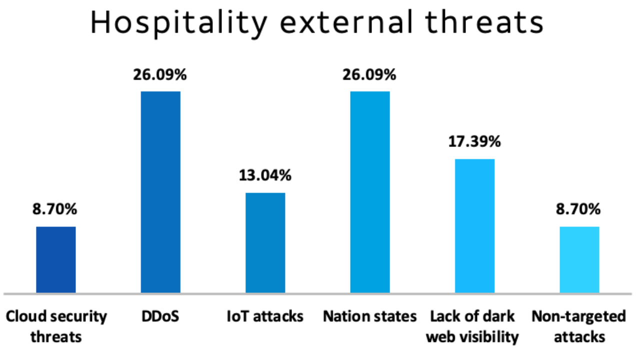
Three Ukrainian nationals have been indicted for the attacks, but there are thought to be a larger group of individuals behind the attacks with links to a number of other criminal gangs.

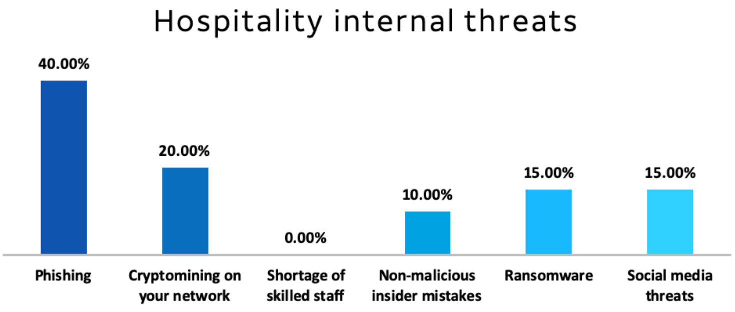
Reports on FIN7 include:

- Carbanak attacks against Chipotle, Baja Fresh and Ruby Tuesday
- The Digital Plagiarist Campaign: TelePorting the Carbanak Crew to a New Dimension
- Footprints of FIN7
- On the Hunt for FIN7

Other criminal gangs also target hospitality, such as AdvisorsBot.

Espionage is also a concern in the hospitality sector. FireEye has reported on an intrusion by APT32 into global corporations, one in the hospitality industry with a plan to expand into Vietnam. While the motivations for this particular attack aren't clear, it's common for some countries to use cyber attacks to gain intelligence on potential commercial partners.





South Korea has also been in the espionage field. A highly sophisticated attacker known as DarkHotel has been known to compromise important hotel guests by installing malware over hotel Wi-Fi hot spots.

AT&T Cybersecurity reported on DarkHotel in 2018, and additional reports on DarkHotel include:

- DarkHotel
- Analysis of the CVE-2018-8373 0day vulnerability attack related to the Darkhotel gang
- Continued DarkHotel Activity
- Asruex: Malware Infecting through Shortcut Files

Russian attackers are also known to target high profile hotel guests, including sniffing traffic on hotel Wi-Fi networks.

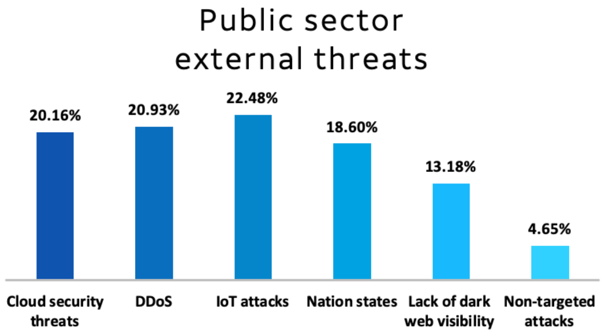
3.3.4 Public sector

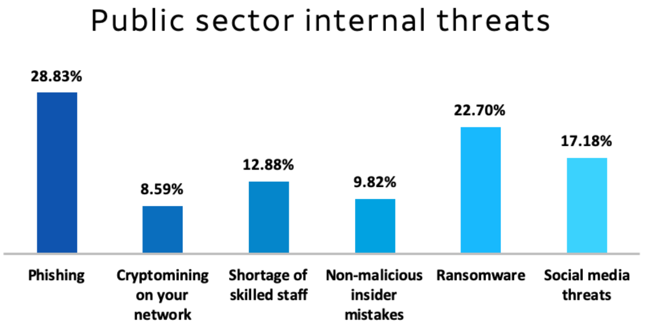
The public sector probably faces the highest level of cyber threats. This is probably why external threats had a pretty equal distribution in terms of nation states, IoT attacks, DDoS, and cloud security threats.

One of the primary attacks the public sector faces is espionage by specific nation hackers.

Attacks against governments by hackers located in China are well documented, as noted in the chart below.

A number of attackers operating from Russia are known to frequently target governments across the world. An infographic from the Estonian government provides an overview that matches the view of the cybersecurity industry.





Some reports broken down into different geographies include:

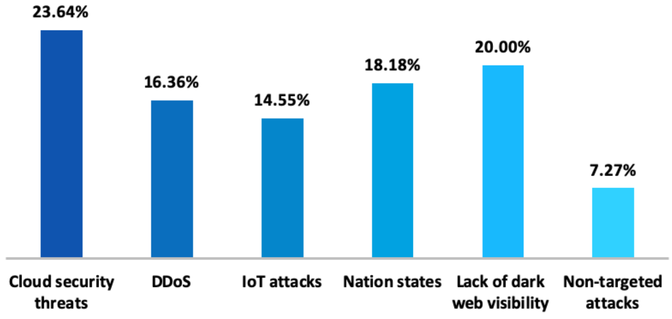
China	• Spear Phishing Techniques Used in Attacks Targeting the Mongolian Government • Tropic Trooper Targets Taiwanese Government With Poison Ivy • Operation Ke3chang Targeted Attacks Against Ministries of Foreign Affairs • The Nettraveler • Chinese Actors attacks on US Government and EU Media
Russia	• 2016 Phishing campaign targeting election officials • Turlas watering hole campaign: An updated Firefox extension abusing Instagram • ThreatConnect Reviews Potential Fancy Bear Activity Targeting the French Election Runoff
Iran	• OilRig Campaign Analysis • Magic Hound Campaign Attacks Saudi Targets • Greenbug cyberespionage group targeting Middle East, possible links to Shamoon
North Korea	• Dissecting Operation Troy: Cyber Espionage in South Korea
Western	• Skywiper • Casper Malware: After Babar and Bunny, Another Espionage Cartoon • The Equation group
Rest of world	• Bahamut, Pursuing a Cyber Espionage Actor in the Middle East • Cyber Attack Impersonating Identity of Indian Think Tank to Target Central Bureau of Investigation • Targeted attack against the Ukrainian military • El Machete Malware Attacks Cut Through LATAM

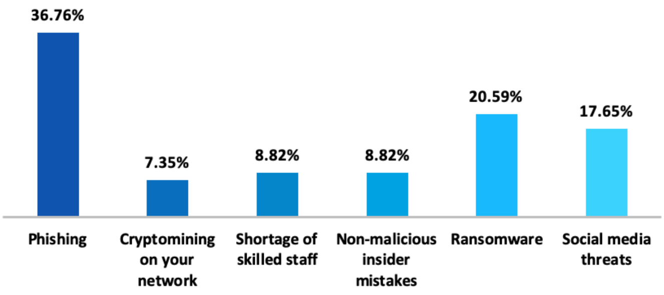
Criminal gain also plays its part in threats to the public sector. SamSam ransomware is a good example and is thought to have earned over $5 million dollars, with local governments and police departments being common targets.

3.3.5 Retail

In recent years, the retail sector has been increasingly targeted. That's probably why targeted external attacks are more of a concern according to our survey. Only 7% cited non-targeted attacks as a worry.

Criminal gain is the main driver here.


Retail external threats


Retail internal threats

PoS Malware
Point of Sale (PoS) terminals have also been targeted with malware, with attacks such as Kronos, ScanPOS, FastPOS, GratefulPOS, UDPoS, Trickbot, FrameworkPOS, and PosCardStealer among the most well known.

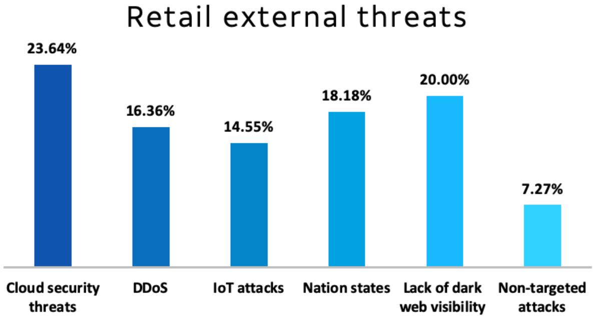
Magecart
A number of large retailers have recently had their websites compromised and malicious code added to steal credit card information from visitors making purchases on the compromised sites.

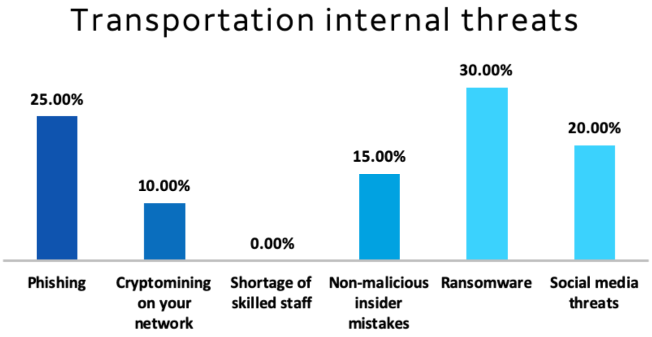
- Inside Magecart
- New Year, Same Magecart
- Newegg - Another Victim of the Magecart

3.3.6 Transportation

Sabotage drives a lot of targeted attacks in the transport sector.

In 2016 attackers naming themselves “1937CN” targeted Vietnamese airlines, defacing flight screens in terminals at Ho Chi Minh and Hanoi airports.





More details on these attacks in OTX:

- Campaign targeting Vietnamese organisations using weaponized Word documents
- Malicious document targets Vietnamese officials
- Goblin Panda targets Cambodia sharing capacities with another Chinese group hackers Temp Periscope

Attackers known as BlackEnergy disabled power systems in Kiev during Christmas 2016 and again in 2017. There’s evidence Black Energy also attempted to disrupt operations at Kiev’s Boryspil airport, and the Ukraine Railway Operator.

BlackEnergy may also be responsible for NotPetya, a destructive worm unleashed against Ukraine that quickly spread across the world and caused billions of dollars of damage.

It is thought to be the most costly cyber attack ever executed. The U.S. Government has named attackers located in Russia as responsible for the attack.

There are many motivations for espionage against transportation, including gaining information on military shipping and logistics.

Reports in OTX include:

- Possible New APT29 Malware
- Operation Dust Storm
- New activity of the Blue Termite APT

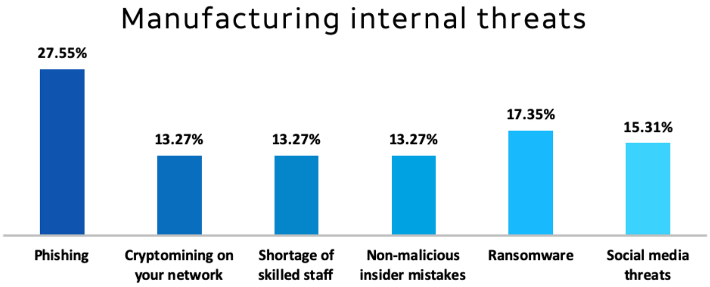
3.3.7 Manufacturing

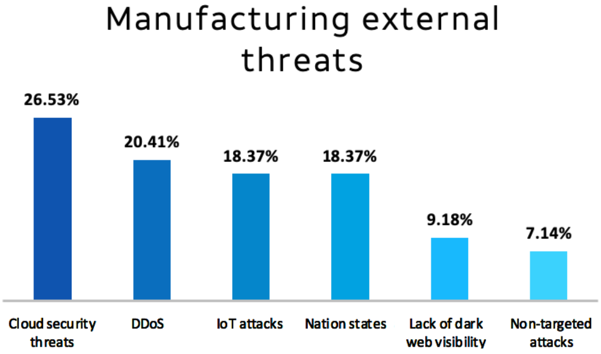
The manufacturing sector faces a range of targeted threats including sabotage, espionage, and criminal gain.

Triton (also known as Trisis) is probably the best known sabotage example. It is an infamous attack framework used to compromise the safety mechanisms of an industrial plant in Saudi Arabia. Disturbingly, the eventual aim of the attack may have been destruction of equipment or even loss of life. The malware targets a vulnerability in Schneider's Triconex Tricon safety system firmware, and can be used to disable key failsafe mechanisms.

The Triton framework was delivered in a traditional network attack—it was only the last phase of deployment that was particular to SCADA (Supervisory Control and Data Acquisition) environments. This also allowed plenty of detection possibilities that were missed at the start of the attack.

While many in the media initially suggested that Iran was a likely source of the attack, due to previous destructive attacks against Saudi Arabia, later forensic evidence linked the development of the tool to researchers in Russia.





The threat of espionage-motivated threat actors against the manufacturing industry is highest for companies involved in the production of technologies with high research costs or with military applications.

Below is a table of where attackers who target the manufacturing sector are likely located.

China	• APT10 • Scanbox
Russia	• Dragonfly
Iran	• IRN2
North Korea	• Duuzer

The threat to the manufacturing sector from targeted criminal attacks, where a particular victim is identified for attack, remains relatively high.

There are a number of organized criminals now targeting manufacturing with ransomware due to the criticality of data and continued operation.

Attackers also target manufacturing companies for the theft of financial data to enable bank thefts, as with any sector.

Reports include:

- FormBook Distribution Campaigns Impacting the U.S. and South Korea
- Defray Ransomware
- Spam Run in Europe Uses Hover Action to Deliver Banking Trojan
- New Vega Stealer shines brightly in targeted campaign
- Attacks on industrial enterprises using RMS and TeamViewer

4. Confidence

Worrying about threats is one thing, but we also wanted to look at the other side of the coin and ask about the level of confidence companies have in their ability to protect, detect, and respond to specific attacks. For this survey, we chose DDoS and IoT attacks.

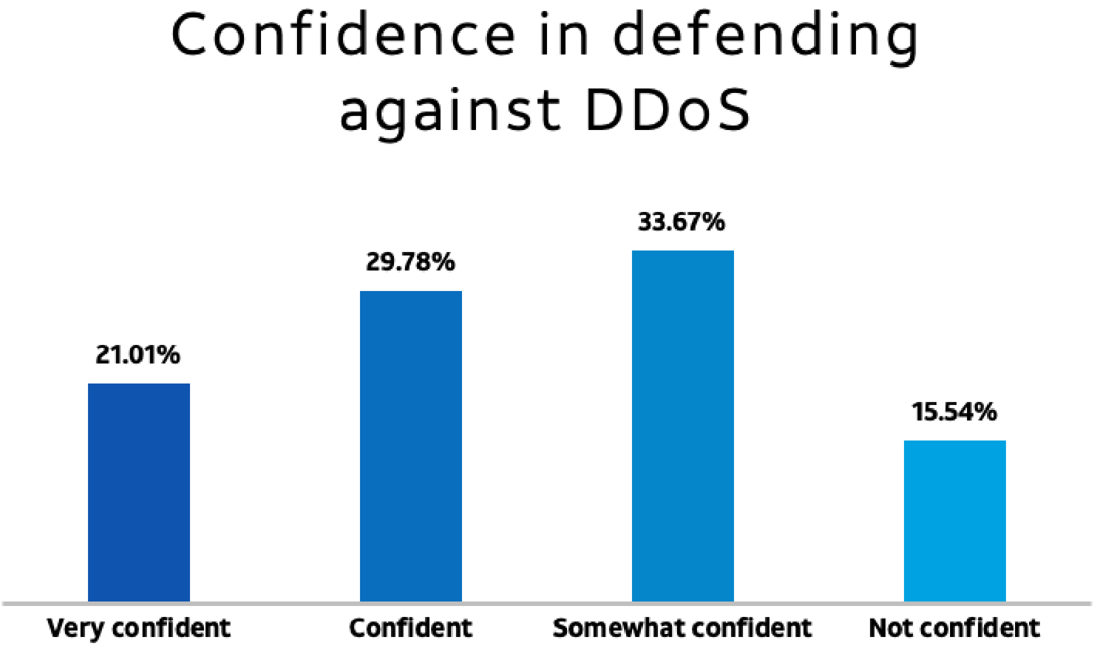
4.1 DDoS attacks

At a broad glance, a third of companies were only somewhat confident in their ability to defend against DDoS attacks. Having said that, around 51% were either confident or very confident in their defensive capabilities.

Only 16% stated they were not confident in being able to defend against DDoS attacks.

When we break the results down by company size, we see that SMBs are far less confident in their ability to defend against DDoS attacks than large companies. Defending against DDoS attacks isn't necessarily cheap, and so, it stands to reason that this is a good example of where investment can buy better security.

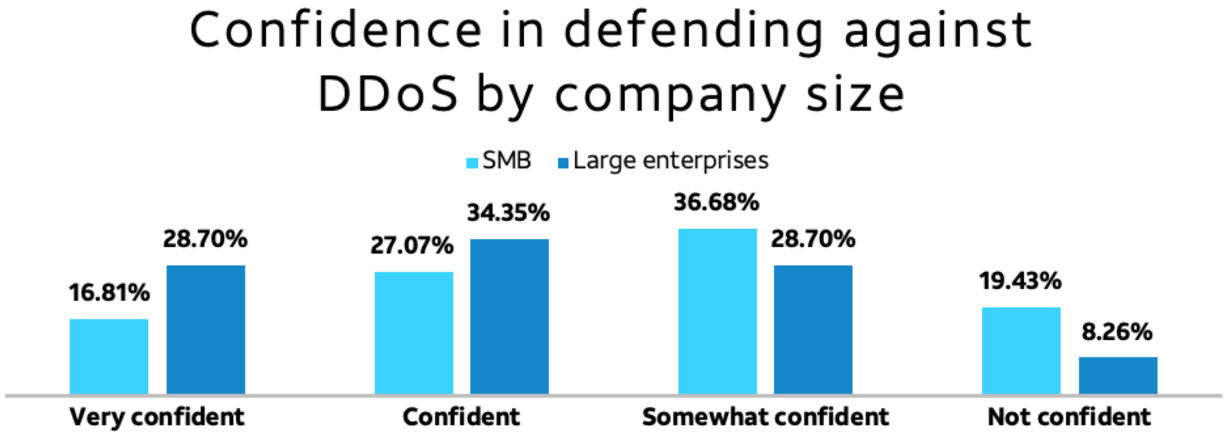
29% of large enterprises were very confident in their ability to defend against DDoS attacks compared with just 17% of SMBs. On the other end of the spectrum, only 8% of large enterprises were not confident, compared to 20% of SMBs.

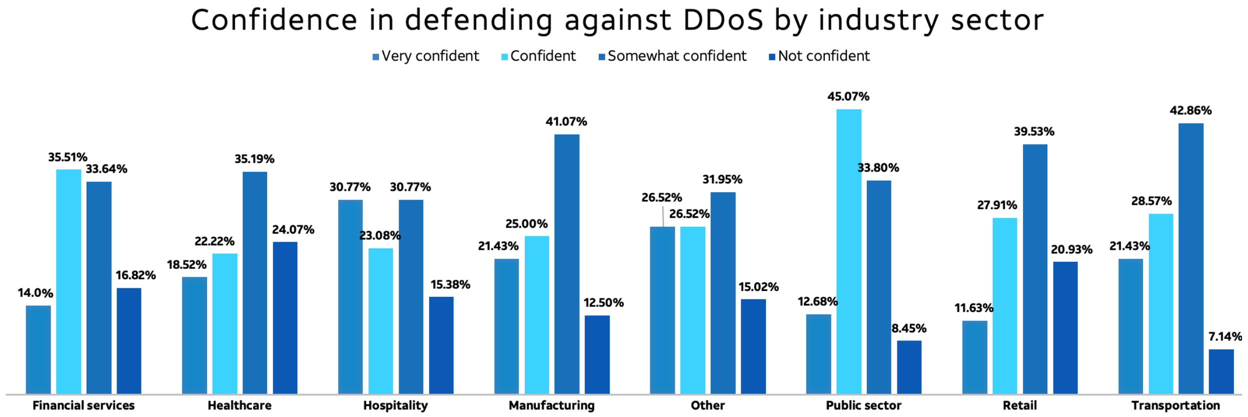


Across the industry, the public sector was the most optimistic, with 45% stating they were confident and 13% stating they were very confident.

Financial services seemed to have a broad spread, with 50% being confident or very confident.

Healthcare fell on the other side of the spectrum with 24% stating they were not confident and a further 35% stating they were only somewhat confident.

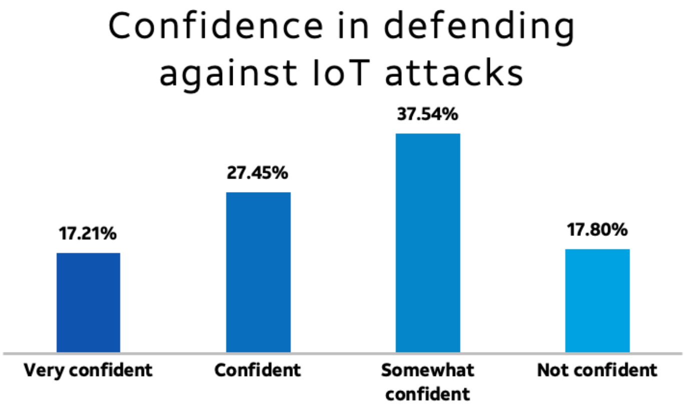

Confidence in defending against DDoS by company size


Confidence in defending against DDoS by industry sector

4.2 IoT attacks

IoT defenses overall mirrored the DDoS confidence levels with 38% of participants stating they were only somewhat confident in their ability to defend against IoT attacks and 18% not confident.

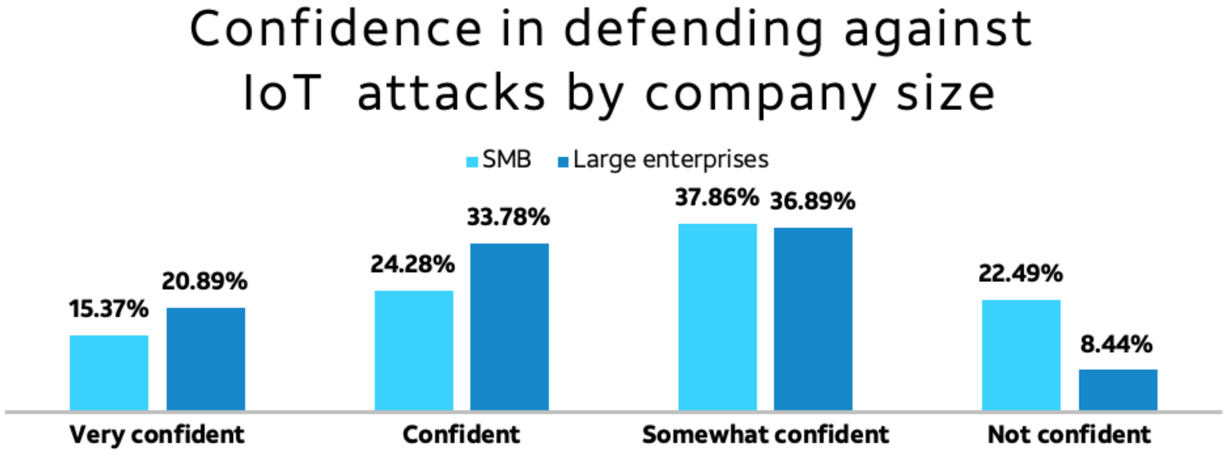
Again, larger enterprises were more confident in their ability to defend against IoT attacks when compared to SMBs.

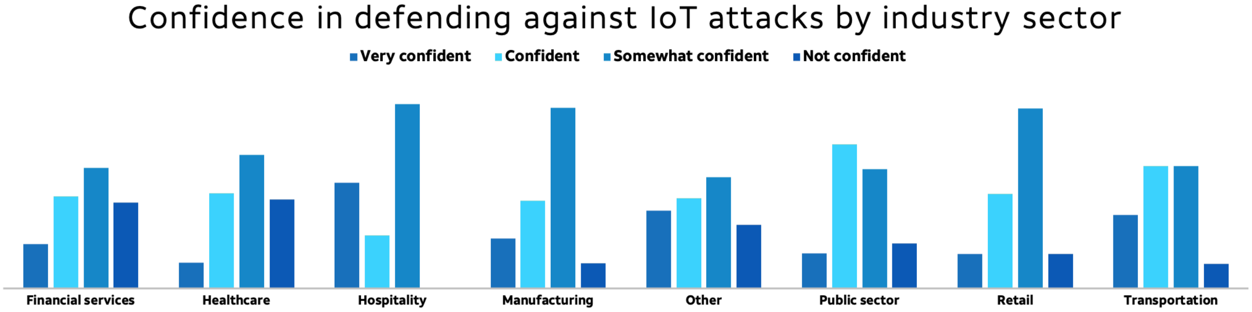

Confidence in defending against IoT attacks

The financial services and healthcare sector had the least amount of confidence in defending against IoT attacks with 25% and 26% respectively responding “not confident.”

Hospitality was perhaps the most polarizing of sectors, with zero participants having no confidence while 54% were somewhat confident and 31% were very confident.

The public sector was on the optimistic side, with 42% stating they were confident, and a further 10% were very confident.





5. Supply chain security

The final question we put to the participants was to gauge their feelings towards supply chain security.

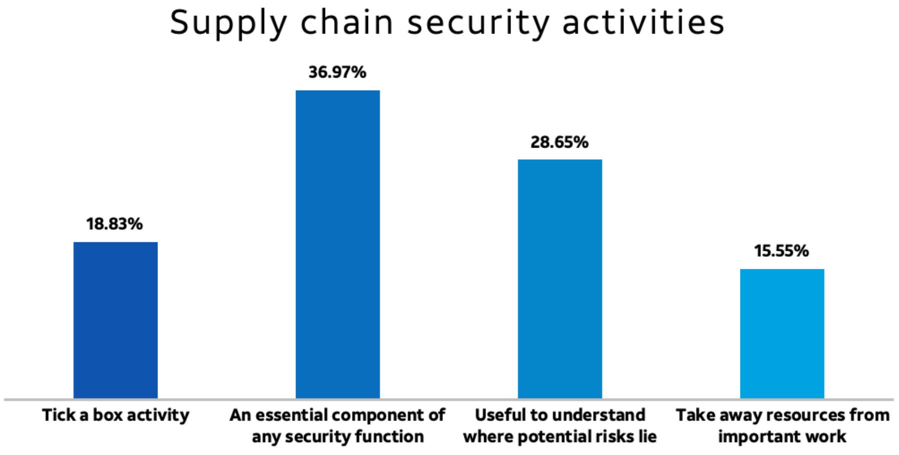
Supply chains have had many column inches dedicated to them over the last few years as many breaches have come to light after a company in the chain was compromised.

With large numbers of credentials being exposed in breaches, credential stuffing has gained more popularity among criminals. This can be viewed as a form of supply chain vulnerability, as one weak vendor exposes credentials that can be used to attack another.

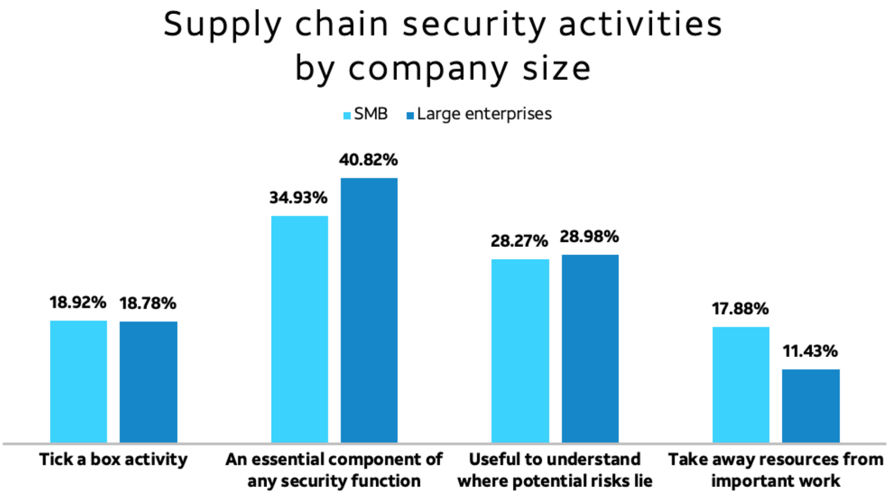
To combat this, enterprises usually undertake a series of supply chain assurance activities. This can take many forms, but typically involves an in-depth questionnaire to third parties asking them to validate their security controls and posture.

Most participants, at 37%, believe that such supply chain security activities are an essential component of any security function. A further 29% believe it's useful to understand where potential risks lie.

While not saying supply chain security activities don't have merit, 16% did say that it took resources away from other tasks, while 19% viewed it merely as a "tick box" activity.



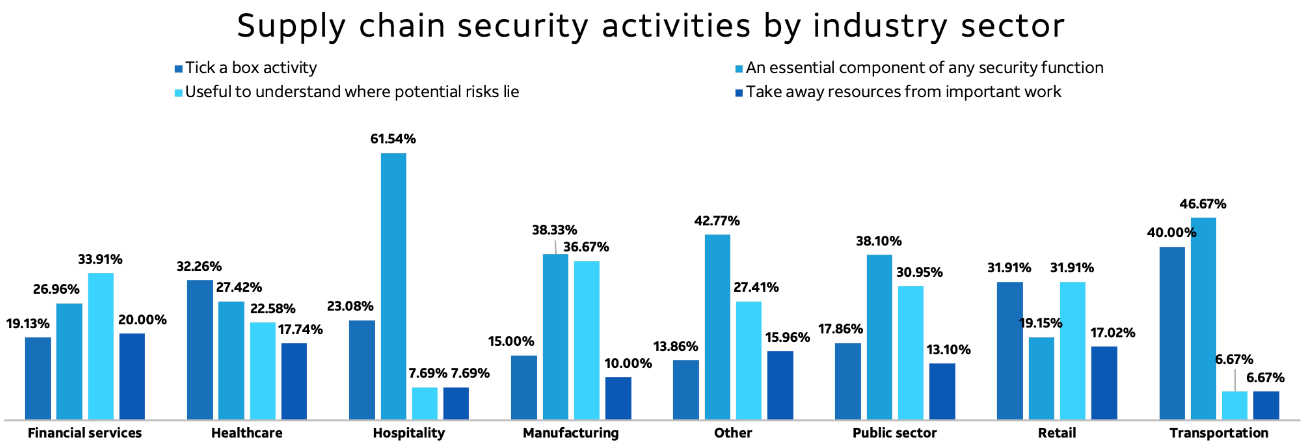
As one would expect, smaller companies viewed supply chain activities as more of a drain on resources than larger companies. This is understandable as smaller companies often don't have a dedicated security team, let alone a department equipped to undertake assurance activities.



Hospitality was the most supportive of supply chain security, with 62% believing it is an essential component of a security function.

47% of the transportation sector also believed it to be important, although within the same sector, 40% believed it to be a tick box activity.

Only 19% of retail sector participants believed supply chain activity to be essential, with 32% stating it was useful to understand potential risks, and another 32% believing it to be nothing more than a tick box exercise.


Supply chain security activities by industry sector

Conclusions

Beneath the aggregated survey results, there are many sub-themes to unpack. And even then, we can’t get the full story, just a version of it.

There is a difference in how large enterprises address security challenges with resources and budget at their disposal compared to smaller-sized businesses. This is evident in the overall confidence companies have in their security capabilities, and where they feel resources get pulled into many directions.

The threat landscape is ever-shifting, and to keep on top of the latest threats requires collaboration with peer companies, robust reporting on system activities, as well as reliable threat intelligence. In other words, situational awareness of the internal and external environment is essential, and while some larger companies may have the capability to do this in-house, most companies do not.

Thought needs to be given not just to the sector a company operates in, but more importantly the size of the company and the amount of resources it has at its disposal. The mid-sized enterprise in particular is being targeted more and more by attackers, yet there are few practical answers to their predicament.

It's not possible to answer this with a neatly wrapped solution with a bow on top. But the following points should be taken into consideration for any company:

1. People

Having the right people can be the difference between being cyber-prepared or not. It doesn't necessarily mean hiring an entire security department. Sometimes, all an organization needs is a consultant to help provide guidance and steer them towards best security practices to ensure security is built right from the beginning.

2. Technology

IT security technologies have come a long way in the last decade. While the constant news cycle may feel like things are getting worse, we actually see more attacks that focus on attacking humans through phishing, or compromises through third parties. Therefore, it makes sense to invest in technologies that offer a broader set of capabilities, especially those which have their own or can integrate with reliable sources of threat intelligence. These can be more affordable, not just to buy, but to maintain on an ongoing basis.

3. Outsourcing

In today's age of the cloud and service providers, in many cases it doesn't make sense to keep everything in-house. Securing the services of a reputable managed security services provider (MSSP) can take away the need to run your own security operation center. Other third parties that can help could include PR agencies and business continuity service providers.

4. Insurance

Finally, where risk can't be mitigated or accepted, consider transferring it to an insurance provider. Not only can insurance help alleviate the financial cost of a breach, but it can go a long way in demonstrating to customers, shareholders, or partners that insurance was part of a broad cybersecurity plan to keep data secure.

Appendix A

The questions

Q1. What size is your organization?

5000 employees or less

Over 5000 employees

Q2. What industry is your organization in?

Financial Services

Healthcare

Hospitality

Manufacturing

Other

Public Sector

Retail

Transportation

Q3. Do you and your (the security team) and execs / stakeholders see eye to eye on cyber risks?

We're completely on the same page

Mostly

Sometimes

Not at all

Q4. How confident are you in your company's ability to detect and protect against DDoS attacks?

Very confident

Confident

Somewhat confident

Not confident

Q5. What external threats worry you the most?

Cloud security threats

DDoS

IoT attacks

Nation states

Lack of dark web visibility

Non-targeted attacks

Q6. What internal threats worry you the most?

Phishing

Cryptomining on your network

Shortage of skilled staff

Non-malicious insider mistakes

Ransomware

Social media threats

Q7. How confident are you in your company's ability to detect and protect against IoT attacks?

Very confident

Confident

Somewhat confident

Not confident

Q8. Supply chain security activities …

Tick-a-box activity

An essential component of any security function

Useful to understand where potential risks lie

Take away resources from important work