softwerx

AT&T Cybersecurity

ALIEN VAULT

The Perception & Reality of Cyber Security Threats

Based on research by our partners AT&T and AlienVault

Introduction

At the recent RSA conference, arguably one of the largest business focused security conferences in the world, AT&T Cybersecurity took the opportunity to take the pulse of the industry.

Between the AlienVault and the AT&T booths they were able find out not only what the feeling is across the industry, but also how it differs based on the size of the organisation.

Outline Method

The report is based on a survey of 733 participants at RSA 2019 and interviews with security experts.

The demographic breakdown is:

<5,000 Employees	5,000< Employees	Total
490	243	733

For the sake of this report organisations with up to 5,000 employees are in the SMB space, while organisations with over 5,000 employees are large organisations.

The original report was written by Javvad Malik, Security Advocate at AT&T Cybersecurity. Any questions about the methodology should be addressed to him directly at jmalik@alienvault.com.

Key Findings

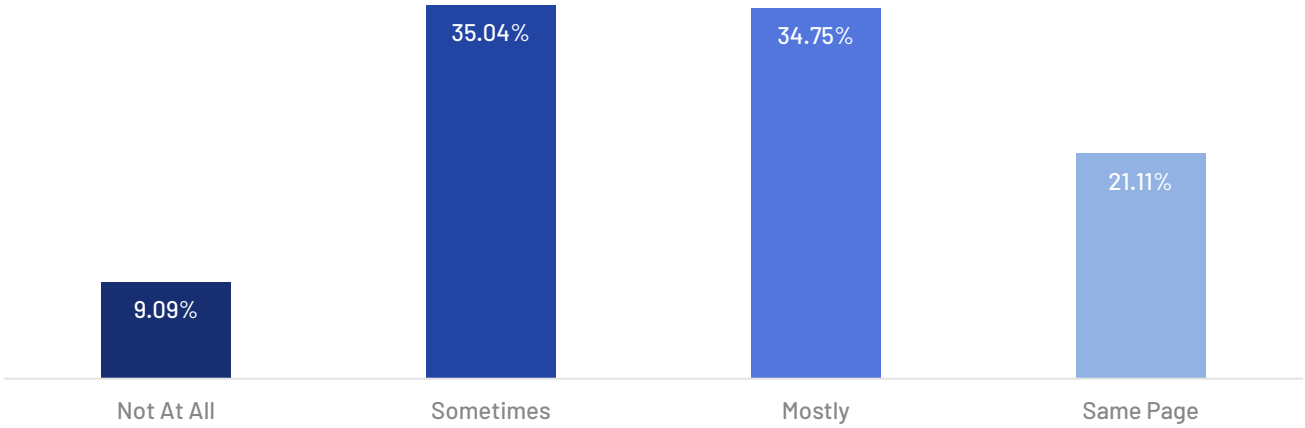
- Large organisations tend to be more aligned with stakeholders.
- The biggest threats that worry organisations of all sizes are phishing (29%) and cloud security threats (27%).
- Only 17% of smaller organisations are very confident in defending against DDoS attacks compared to 29% of large organisations.
- Only 15% of smaller organisations are very confident in defending against IoT attacks compared to 21% of large organisations.
- Most organisations view supply chain security as an essential component of any security function (37%). Though 18% of smaller organisations still feel these activities take away resources from important work, and 19% believe it's just a "tick box" activity.

Seeing Eye to Eye

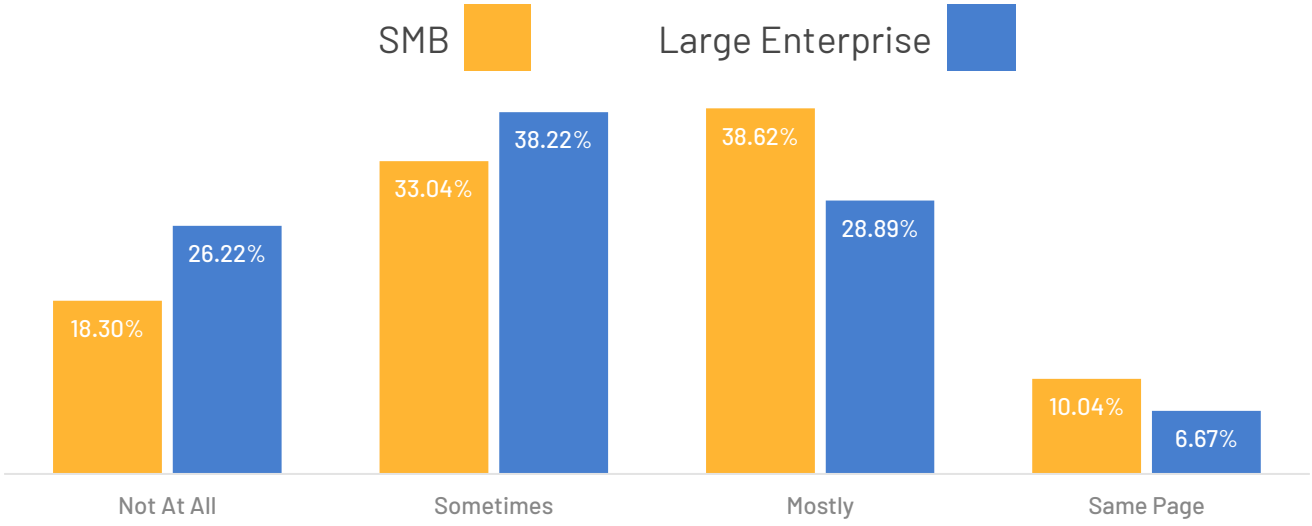
Do you and your (the security team) and execs / stakeholders see eye to eye on cyber risks?

- We're completely on the same page
- Mostly
- Sometimes
- Not at all

Totals Across All Sectors:



By Business Size:



Overall, the results form a standard bell curve - most responses falling in the middle of the spectrum.

When the results are split by organisation size, a different picture emerges.

Larger organisations appear to have a far better alignment with their stakeholders than small or medium organisations (SMBs).

Stakeholder alignment is a vital part of your cyber security posture. Without it budgets can be cut, resources limited or inappropriately applied and active engagement across the business will be difficult to achieve.

Key elements of your strategy need user buy in across your organisation; security awareness training and phishing prevention are reliant on your staff and supplier due diligence needs to be applied consistently even on small purchases.

Unauthorised hardware use and firewall 'workarounds' that might allow staff to access sites that have been blocked for a reason are much easier to avoid if everyone is on the same page.

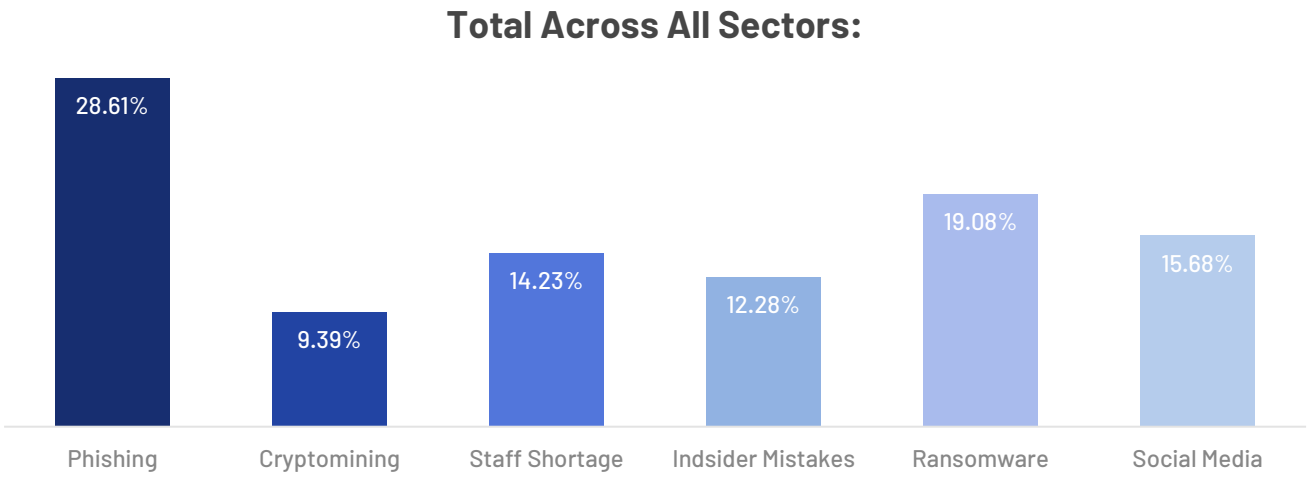
A key element of securing the kind of buy in you need from the top of your organisation lies in reporting. Having clear, accessible, accurate statistics on threats avoided, threats not avoided, where they came from and why could be your greatest asset in budget meetings.

Threats

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

What internal threats worry you the most?

- Phishing
- Cryptomining on your network
- Shortage of skilled staff
- Non-malicious insider mistakes
- Ransomware
- Social media threats



There was very little differentiation between larger and smaller organisations.

Phishing

Nearly a third of organisations put phishing as the threat that worries them the most.

Phishing is sending emails pretending to be from reputable organisations asking people to send personal or business information, such as passwords and credit card numbers or a asking them to click a hyperlink, which would download a virus.

Phishing is a threat to organisations on two fronts – there is the risk that someone could imitate a supplier or donor and persuade your staff to send data or payments somewhere they shouldn't.

There is also the risk that someone could breach your email defences and find a way to imitate you. By emailing your donors as if from your domain they could convince them to send donations or data somewhere they shouldn't.

It is likely that the root of this fear of phishing lies in the fact for most cyber threats, a technology solution is available to protect you, but with phishing most systems rely on your staff being able to detect and respond appropriately.

Ransomware

In second place comes ransomware. You can't hide the fact that your systems have been compromised and even if recovery is quick without any loss of data, the damage to your reputation can be significant.

Social Media

Social media threats showed up in third place. The rapid rise of social media has become a sort of wild west where many organisations are struggling to manage and chart sources of risk.

Worse still any mistakes are likely to be public and can impact brand and trust, expose sensitive information, or become a source of entry into an organisation.

Non-Malicious Insider Mistakes

A non-malicious insider threat is a staff member who intentionally breaks policies, but without the intent to do harm.

They create the biggest vulnerabilities when paired with a malicious intruder. One person may have an intent to steal data, but their well intentioned colleagues who provide them with access to data they shouldn't to help them 'do their job'? They are just trying to help productivity, but they can make the problem 10 times worse.

Education is the key here. Your staff need to understand why policies are in place and what the risks are of breaking them, otherwise they may seem like a bureaucratic barrier to efficiency.

Effective log management is a great foundation for this education process, being able to show staff actual, or even real time, risks and consequences makes the lessons stick.

Shortage of Skilled Staff

The NSCS has recently concluded that the gap between the demand and supply of skills in the top tiers of cyber security is now verging on crisis point.

A cyber security skills gap of some degree is inevitable in an industry where skills development must try to keep pace with the extraordinary rate of technological change, but the issue goes well beyond that.

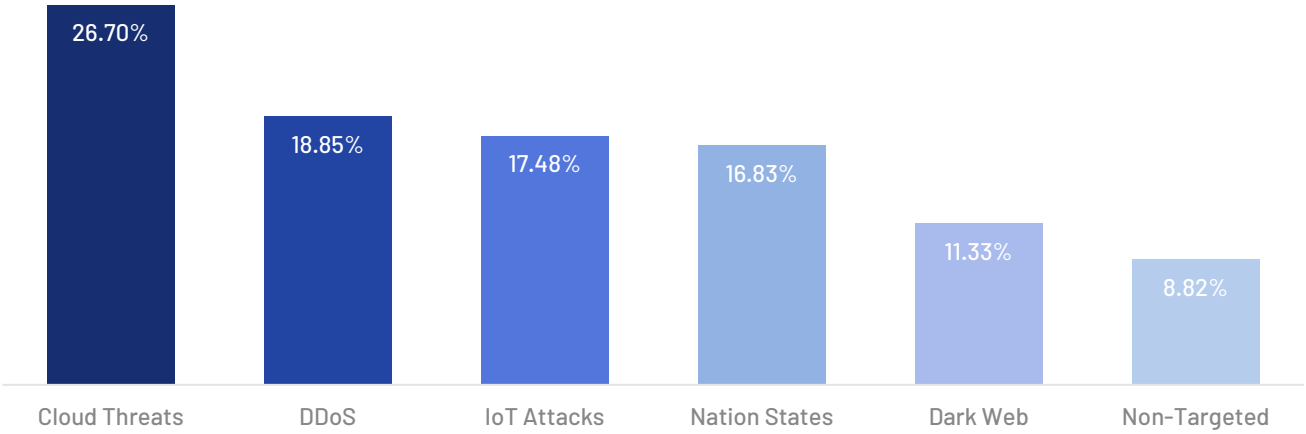
Cryptomining

Cryptomining is the process of solving complex problems to verify digital transactions using computers. Miners either create a cryptocurrency or get paid for their processing power in a cryptocurrency like Bitcoin. When used maliciously an attacker will plant a cryptomining code to your network and hijack your processing power for their own purposes, slowing your operations down and providing a back door for other attacks.

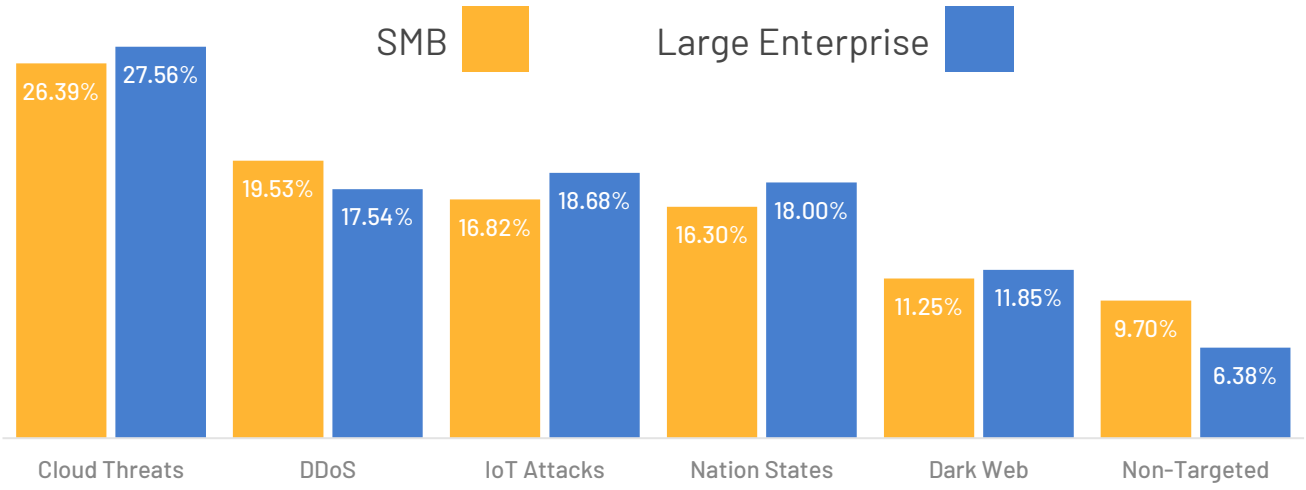
What external threats worry you the most?

- Cloud security threats
- DDoS
- IoT attacks
- Nation states
- Lack of dark web visibility
- Non-targeted attacks

Total Across All Sectors:



By Business Size:



Cloud Security

Cloud security threats were cited as the most worrying in 27% of all responses. It is still a relatively new area for many organisations.

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, organisations are right to be worried.

DDoS

In second place a distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as your server, website or other network resource.

They send a flood of incoming messages, connection requests or malformed data packets to the target system forcing it to slow down or even crash and shut down, denying service to legitimate users or systems.

IoT – Internet of Things

In a close third the internet of things is a relatively new concept, where items that may not even have had a circuit board before are now connected to the internet. At home it may be your toaster, your oven, or your heating system.

Whilst the wider application in business has started more in the manufacturing and transport industries you aren't immune in an office.

If you have on site servers and a smart cooling system, your whole network could be damaged. If your entry control system is connected to the internet an attack could let the wrong person in or lock your legitimate staff out.

Nation States

Even for charitable organisations many attacks will fall under two categories - criminal gain or sabotage, which have several active groups and nations.

North Korea, Russia and China can all be considered as significant threats, with reports the governments have attempted to steal billions in data and money in aggressive attacks.

Having mobile staff spread out nationally or internationally only makes a good cyber security posture harder to attain.

Lack of Dark Web Visibility

Fewer organisations rated this issue as important overall.

However, maintaining visibility into the dark web is an important part of your cyber security posture. You need to know if some of the stolen data being sold on the dark web is yours.

Non-Targeted Attacks

Non-targeted attacks are at the bottom of the list of concerns. For big business they are less scary than someone who has done their homework and found a weakness in their organisation.

But more general attacks seeking to exploit a known software weakness and pick up anything of value left vulnerable from any user it can could to a lot of damage and are more likely for smaller organisations.

It is vital that your cyber security posture includes a rigorous patch management scheme to make sure known vulnerabilities are patched as quickly as possible.

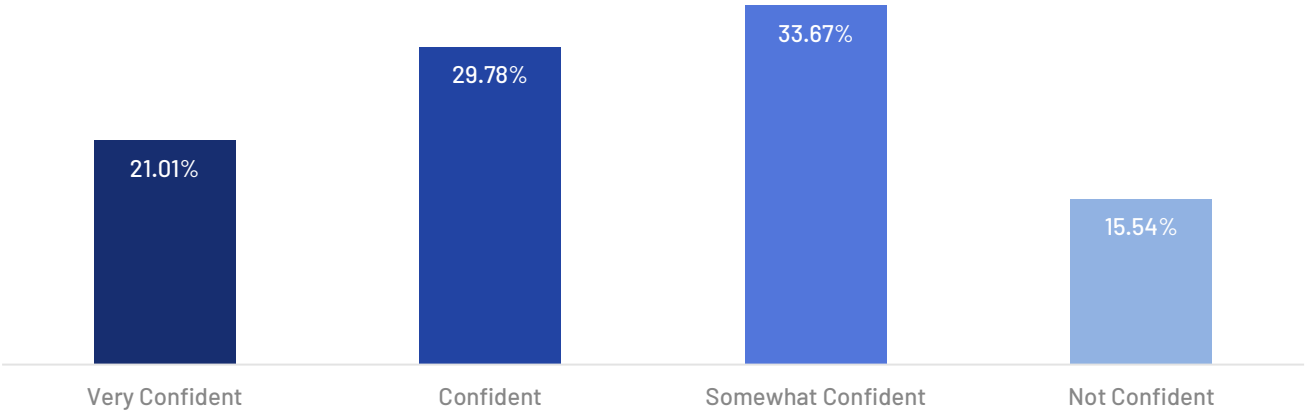
Confidence

The survey wanted to look at the other side of the coin as well. They asked respondents about the level of confidence they have in their ability to protect, detect, and respond to DDoS and IoT attacks.

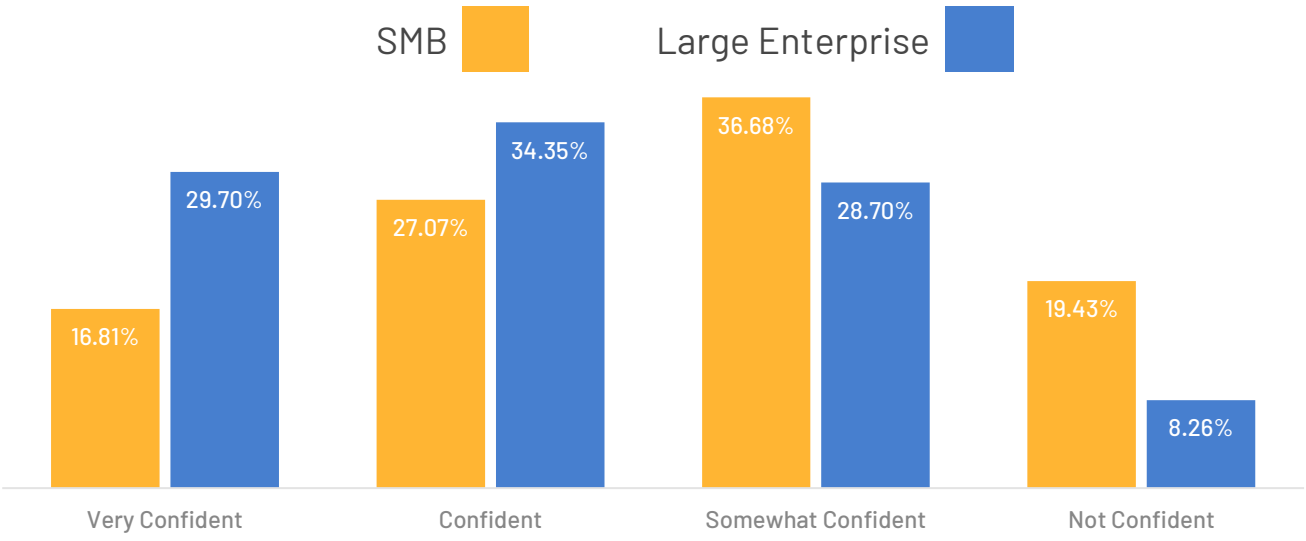
How confident are you in your organisation's ability to detect and protect against DDoS attacks?

- Very confident
- Confident
- Somewhat confident
- Not confident

Total Across All Sectors:



By Business Size:



DDoS attacks are common where hackers or hacktivists want to disrupt activities or damage reputations rather than seeking access to specific data. Despite the higher likelihood of facing such an attack, around a third of respondents where only somewhat confident of their abilities to defend against such an attack.

However, around 51% of respondents were either confident or very confident in their defensive capabilities.

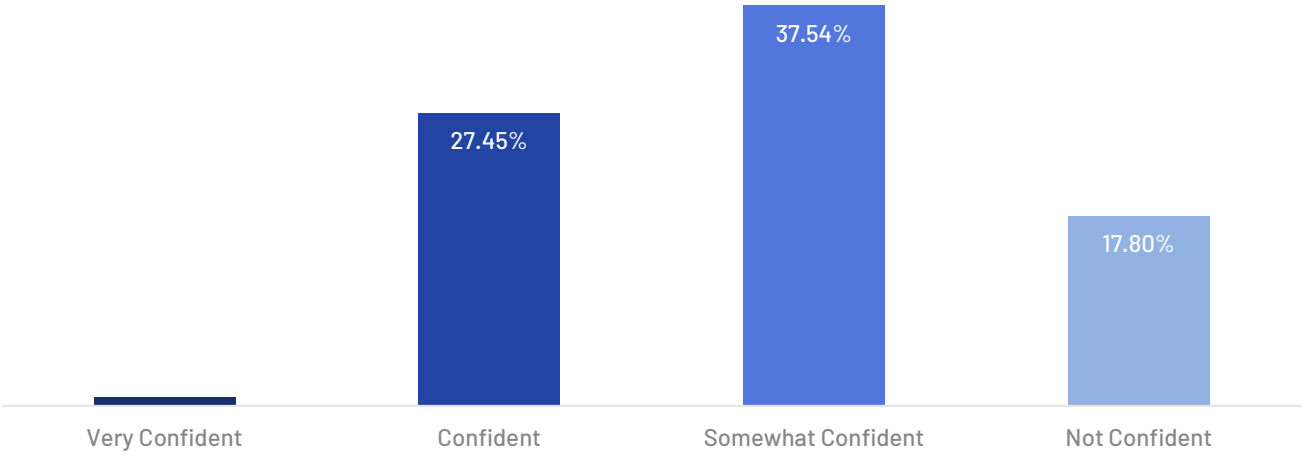
Smaller organisations are far less confident in their ability to defend against DDoS attacks than large organisations. Defending against DDoS attacks often costs a fair bit so this is a good example of where investment can buy better security.

29% of large organisations 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 organisations were not confident, compared to 20% of SMBs.

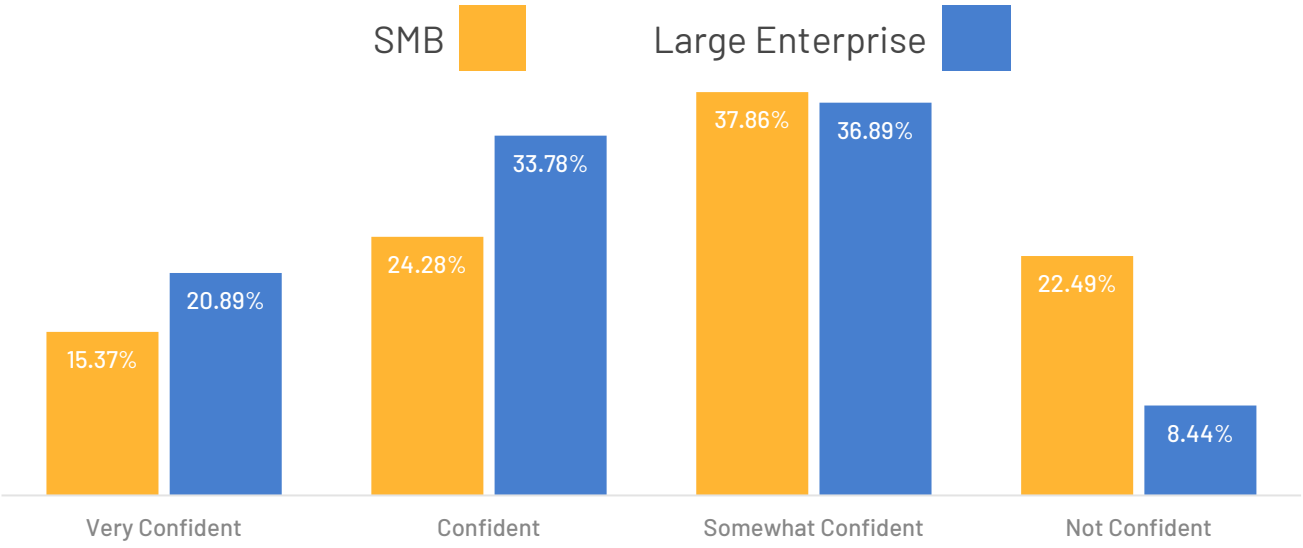
How confident are you in your organisation's ability to detect and protect against IoT attacks?

- Very confident
- Confident
- Somewhat confident
- Not confident

Total Across All Sectors:



By Business Size:



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

softwerx

AT&T Cybersecurity

ALIEN VAULT

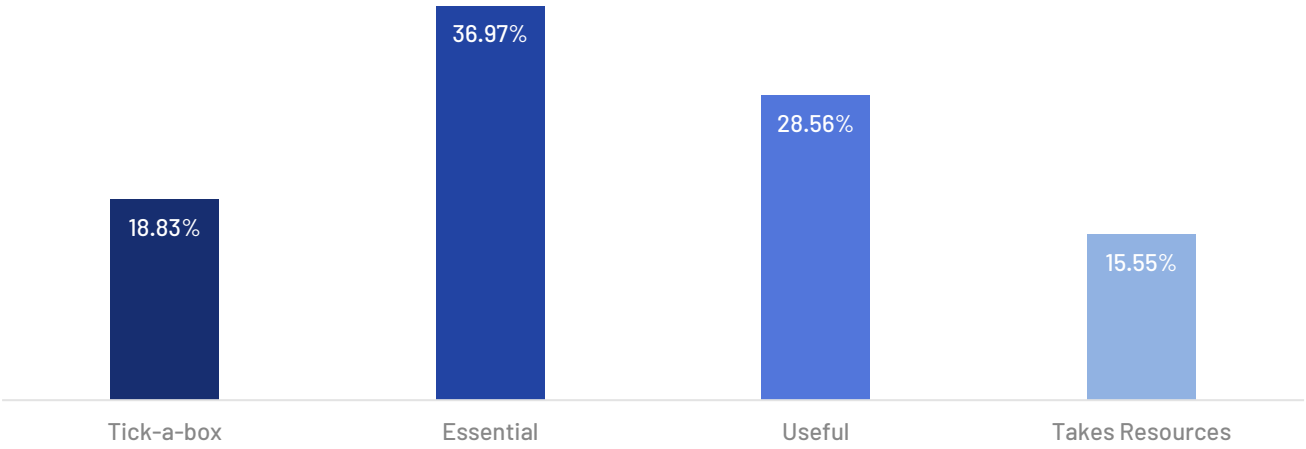
Supply Chain Security

Many breaches come to light after an organisation in the chain was compromised, one weak vendor can expose credentials that can be used to attack you. It continues out in the chain, one breached supplier, originally attacked through their supplier could also be used to attack you.

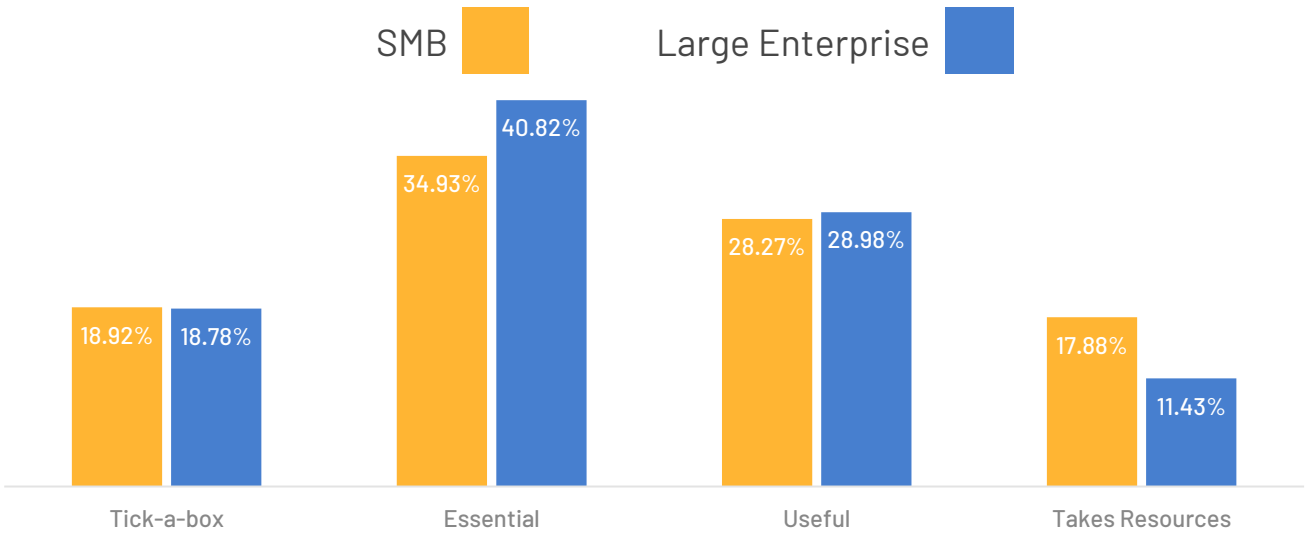
Supply chain security activities...

- Are a tick-a-box activity
- Are an essential component of any security function
- Are Useful to understand where potential risks lie
- Take away resources from important work.

Total Across All Sectors:



By Business Size:



To combat supply chain vulnerabilities, organisations undertake a series of supply chain assurance activities as part of their due diligence. Typically, it 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.

Smaller organisations viewed supply chain activities as more of a drain on resources, which is understandable as they often don't have a dedicated security team, let alone a department set up to handle the security side of due diligence.

Conclusions

There's a difference in how large organisations with resources and budget at their disposal feel about security challenges compared to smaller-sized organisations. This is evident in the overall confidence organisations have in their security posture.

The threat landscape is constantly changing, and to keep on top of the latest threats needs collaboration with peer organisations, robust reporting on system activities, and reliable threat intelligence. Situational awareness of your internal and external environment is essential and while some larger organisations may be able to handle monitoring inhouse, most can't.

Having the right people can be the difference between being prepared or not. Not everyone needs an entire security department. Sometimes what you need is a consultant to help provide guidance and steer you towards best security practices and ensure your security is built in from the start.

IT security technologies have come a long way in the last decade. In response to this more attacks focus on attacking humans through phishing, or compromises through third parties. This makes threat intelligence and monitoring a vital component of cyber security.

It has to be accepted in the modern world that you can never prevent all cyber attacks. The key is to reduce risks, and where risk can't be mitigated or accepted, you may want to 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 is part of a broad cyber security plan to keep data secure.

As well as outsourcing risk, you may want to outsource management. In the age of the cloud and service providers in many cases it doesn't make sense to keep everything inhouse. Cyber security isn't your core business, so outsourcing to a firm where it is a core competency will often get you a better solution for far less than trying to recruit directly.