ALIEN VAULT
An AT&T Company

BLACK HAT 2018 SURVEY REPORT

Extortion, the Cloud, and the Geopolitical Landscape

Table of Contents

1. Executive Summary

1.1 Introduction

At Black Hat 2018, we surveyed attendees on diverse topics ranging from how to react to extortion, what impact the geopolitical landscape is having on the industry, and whether the shiny veneer of the cloud is beginning to fade.

1.2 Key Survey Findings

- 38% say the Chief Information Security Officer (CISO) should be the one to negotiate extortion and/or ransom demands
- 46% of those surveyed say security remains the biggest blocker to cloud adoption
- 54% of participants believe US public sector infrastructure is either unprepared or very unprepared to defend against cyber attacks

1.3 Methodology

This report is based on a survey of 963 participants at Black Hat 2018 and interviews with security experts. This report was written by Javvad Malik, Security Advocate at AlienVault, an AT&T Company. Any questions about the methodology should be addressed to him directly at jmalik@alienvault.com.

2. Reputation, Attacks, and Negotiations

Reputation risk has been well-documented in enterprises for many years. It has often served as a catch-all to try and quantify the impact where a cash value cannot be accurately assigned.

For example, the defacement of a marketing website may not cause any direct financial impact beyond the incident response costs, but there is a reputational cost that needs to be taken into consideration.

So, while reputational damage has always been well-understood, it's the more recent rise of social media, and the speed at which news travels, that has made it more of a risk.

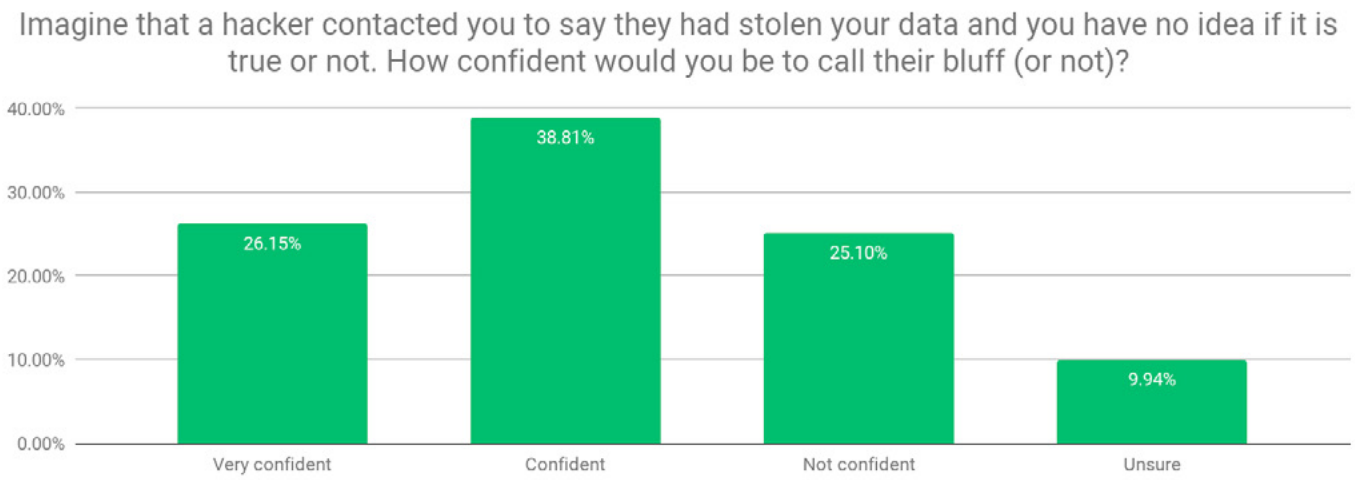
The takeover of corporate social media accounts by attackers, and/or disgruntled (re recently fired) employees is perhaps the most visible and commonly-seen example of a reputational attack on a company.

But a reputational attack doesn't always need a visible output. The mere indication that a company has been breached can be enough to get the rumor mills engaged, regardless of the truth.

Consider the scenario where a company is publicly contacted by an unknown party that states it has breached and stolen its customer database. What would, or should be the response? How confident does a company need to be in order to call the scammer's bluff – maybe the scammer doesn't have any data at all?

More than half of the participants surveyed stated that they were either confident (39%) or very confident (26%) in their ability to verify whether claims were true or false.

However, 25% of participants stated they were not confident in their ability to ascertain whether data had been stolen or not. While 25% may seem like a high percentage, it's quite consistent with the number of incidents where the true extent of the breach is discovered many months later.



Raj Goel, CEO of Brainlink International, and renowned security and privacy professional, shared his views on how he would handle this scenario in the capacity of his role as CEO:

As a small company, I'd ask them to:

1. Provide proof that they have the list [customer database]

2. Determine the origin of the information and consequential risk factor

- **Company website** – *If the client list was pulled from our website, an email marketing platform, and/or LinkedIn; I don't care, because [the database they have] is only names and email addresses, and risk is effectively at zero. CRM system – If the data came from our CRM system, I would be concerned and would need to know the type of data that they had:*
  Names and emails?
  Billing details?
  Systems inventory?
  This raises my internal threat/risk meter from 10 to 50 percent.
- ***Knowledge wiki*** – *If the data came from our knowledge wiki – ouch – now our risk has increased to 80 percent because that contains sensitive data.*
- ***Password manager*** – *If the data came from our password manager – now our risk is at 100 percent and I am at their mercy completely.*

After determining the origin and completing my risk assessment, I would consult with colleagues and friends in the InfoSec community to determine whether the threat is real or fraudulent.

Summary:

As a CEO, I would negotiate. If the threat is real, I would loop in my legal counsel AND my insurance agent. If the risk is over 75 percent, then my team and I would look into engaging third party experts in order to conduct forensics, close doors, etc. My first instinct will always be to have the 'hacker' prove the validity of the data and provide 'proof-of-life.'

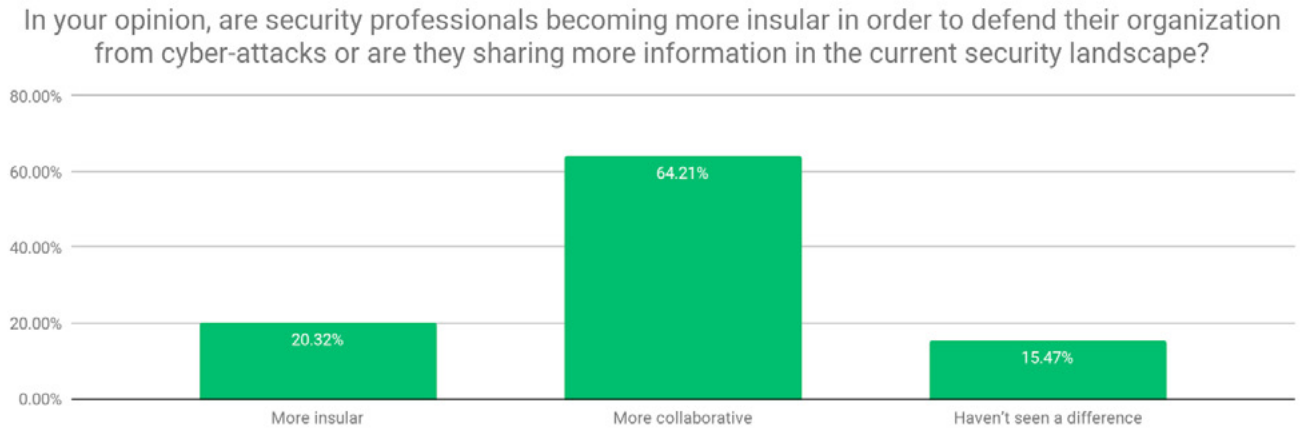
So who should be responsible for making decisions when negotiating with hackers or extortionists demanding a ransom? 38% of the participants believed it should be the CISO, 23% chose the Head of the IT Department, and 18% felt that the responsibility should fall on executive personnel.

It's not surprising to see the CISO at the top of the list. In this role, s/he will usually be best placed to understand the attacker's demands. The CISO has inside access to tools and resources enabling him or her to not only determine the legitimacy of the claims, but also understand the regulatory and business impact should the claims be legitimate.

But, does that mean the CISO should also be the one doing all the negotiating? Perhaps a more collaborative approach like the one Goel indicated, stating he would loop in legal counsel, insurance agents, and third-party experts depending on the level of risk.

Dan Cuthbert, Global Head of Cyber Security Research at BANCO SANTANDER believes that C-level and general counsel support is needed, as well.

"Firstly, you have to verify what is being said. Is the person credible? Are they known for this? Is this a pre-cursor for an extortion attack? You have to validate all as this is vital. C-level should engage with general counsel support."

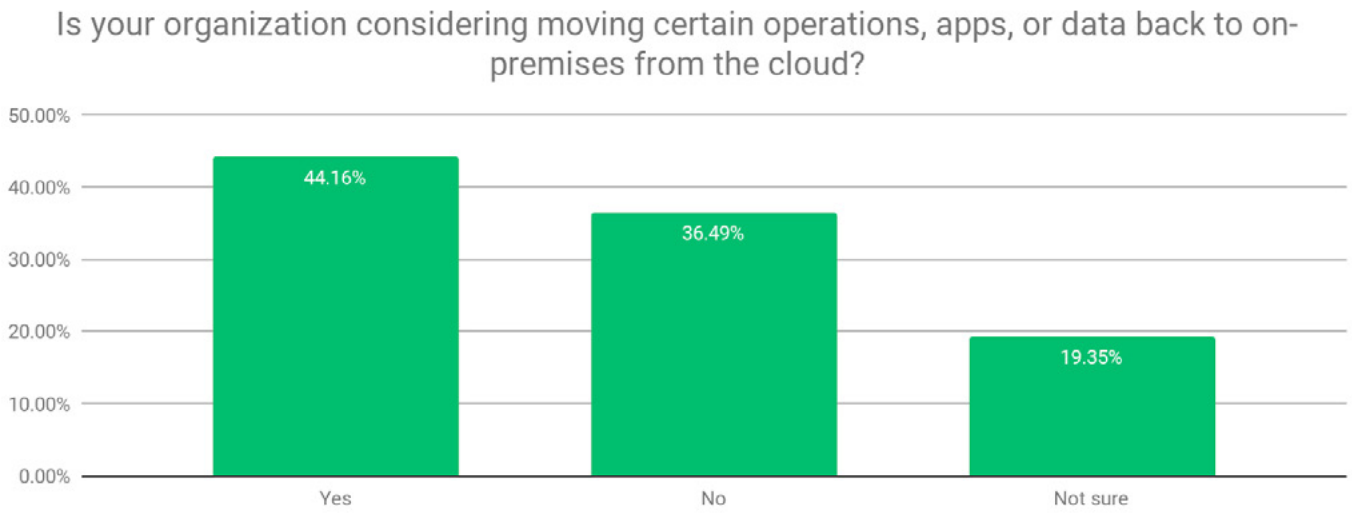


When discussing attacks, it's important to bear in mind the collaborative nature of attacks and how defense also relies on collaborative measures. In fact, to see the vast majority of participants stated that they believe security professionals are becoming more collaborative in their efforts to secure enterprises.

3. Cloudy with a Chance of Pitfalls

The cloud has grown in both influence and the range of deployment for both enterprises and consumers, alike. The cloud isn't just for backing up and synchronising data; it serves as a platform from where many applications are hosted and deployed from.

However, like most innovations, we witnessed a period of a "cloud rush" – businesses were swayed by promises of elastic storage, reliable infrastructure, and cheaper operating costs. Many voices of reason for security, or otherwise, were quickly silenced as naysayers.



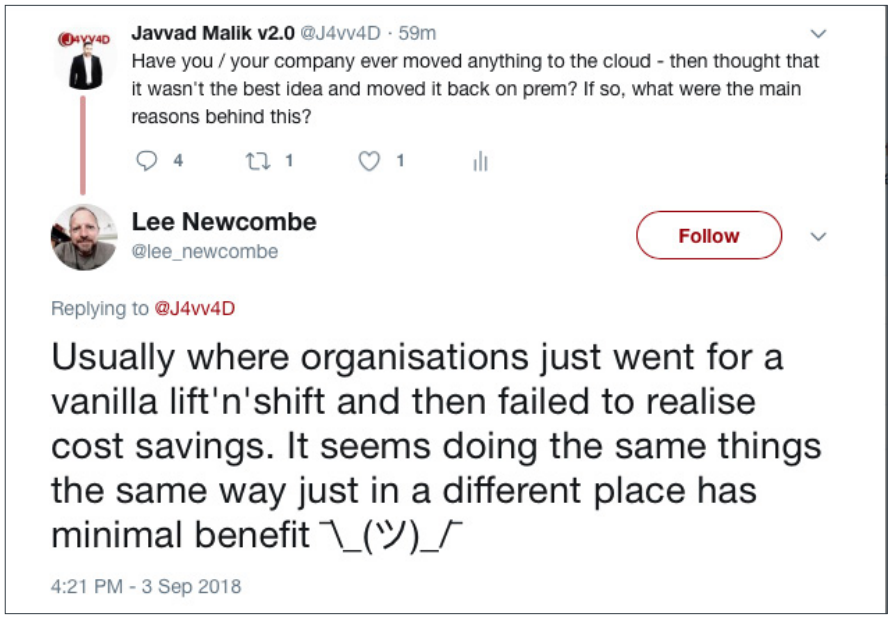
Now, with several years of cloud experiences behind us, it felt like a good time to ask whether the cloud "promised land" was all that it was believed to be.

44 percent of participants claimed that their organizations were considering moving certain operations, apps, or data back to on-premises from the cloud.

Does that mean that the cloud is not all that it's cracked up to be? Not really – it more than likely means that full consideration wasn't given to all the aspects of cloud prior to migration.

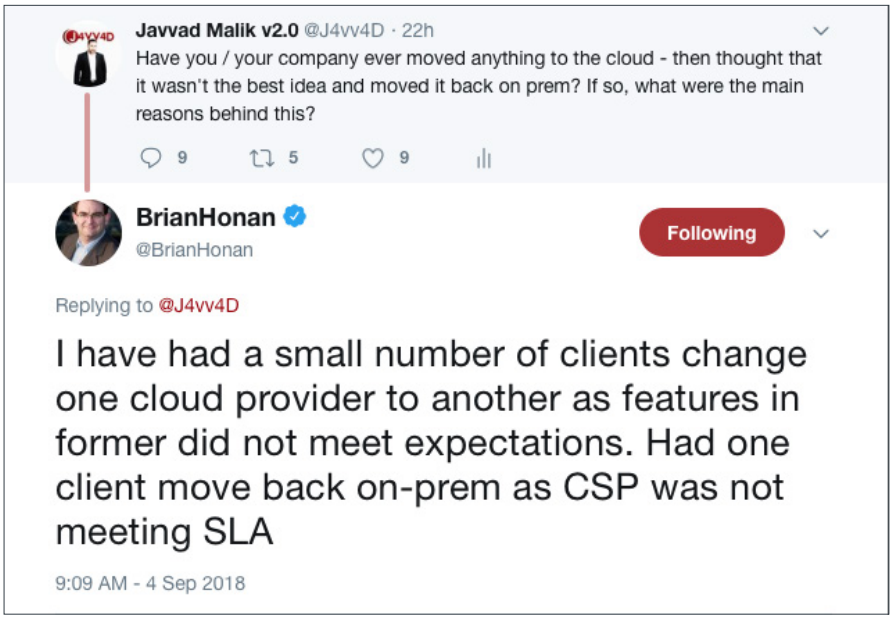
As @RMGirlUK stated on Twitter, "sometimes, the cost analysis isn't conducted up front. "

Lee Newcombe raised an important point about how simply lifting and shifting workloads into the cloud isn't the solution, and can incur additional costs overall.

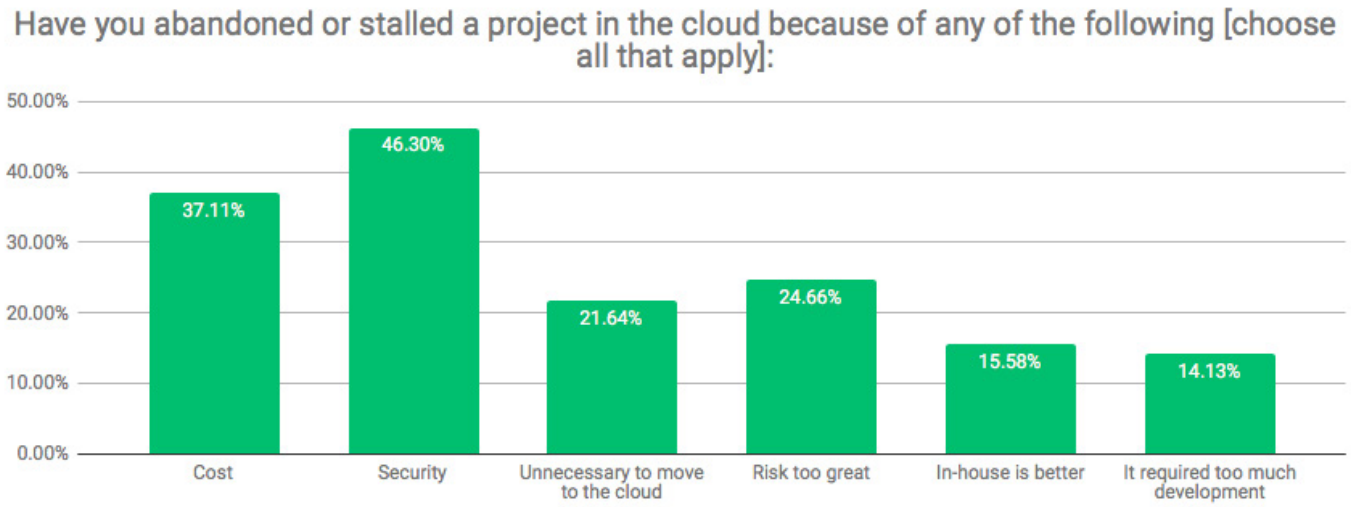


Quentyn Taylor also highlighted the point that for many companies, the cloud is a one-way street, with little thought or planning put into what to do if they want to change environments.

Brian Honan observed with some of his clients that sometimes performance is actually the main issue.



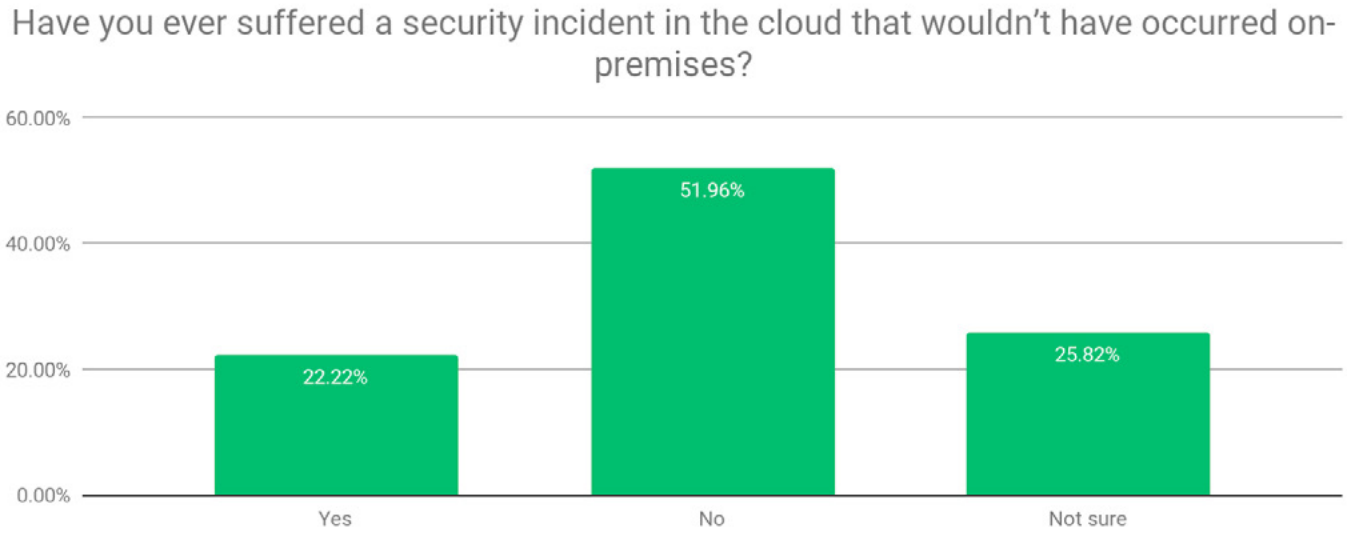
Sometimes companies don't even make it to the cloud before their project is stalled or abandoned. Security, at 46% topped the list of reasons for stopping a project while cost came in second place at 37%. This survey didn't delve into whether it was the cost of actually running in the cloud, or the cost needed to migrate to the cloud that made the project prohibitive, but 14% attributed the large amount of development required to migrate to the cloud as the factor.



While these stats may portray the cloud in a negative light, this does not reflect majority public opinion. It is this surveyor's opinion that the cloud remains a good, stable, and cost-effective platform for many companies. The risks are different, as are some of the operating procedures. The architecture needs to be planned differently, and the cost breakdown works differently, as well. Companies that are considering a move to the cloud should weigh all of the different options, and figure out what works best for their organization, prior to making the commitment.

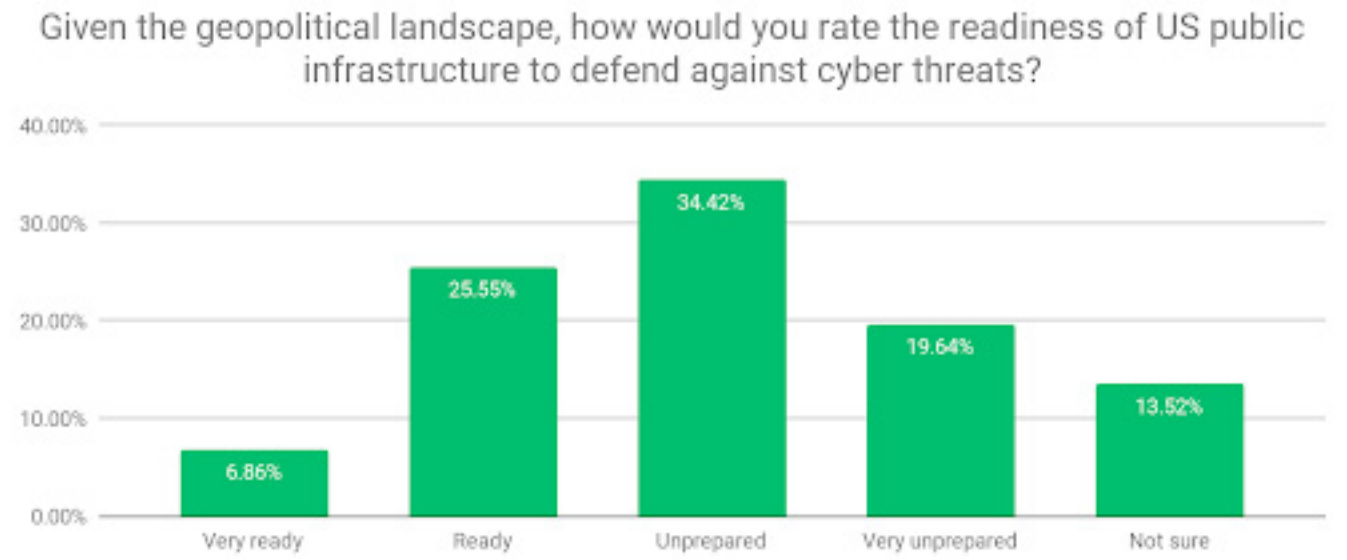
For example, there are some security threats that exist in cloud environments more so than on premises. So, threat detection rules that worked on premises may need to be updated to encompass cloud threats, or at the very least, ensure that systems can import and normalize cloud logs.

Speaking of the difference between threats in the cloud vs on premises, we asked participants whether they had ever suffered a security incident in the cloud that would not have occurred on premises. The majority of respondents, at 52% didn't believe any incident had occurred in the cloud which wouldn't have occurred on premises, while 22% said that such an incident had taken place. While no-one would go on record to describe incidents that were cloud specific, one can assume that the majority of such incidents would be cloud-specific, such as misconfigured databases, or private keys published publicly.



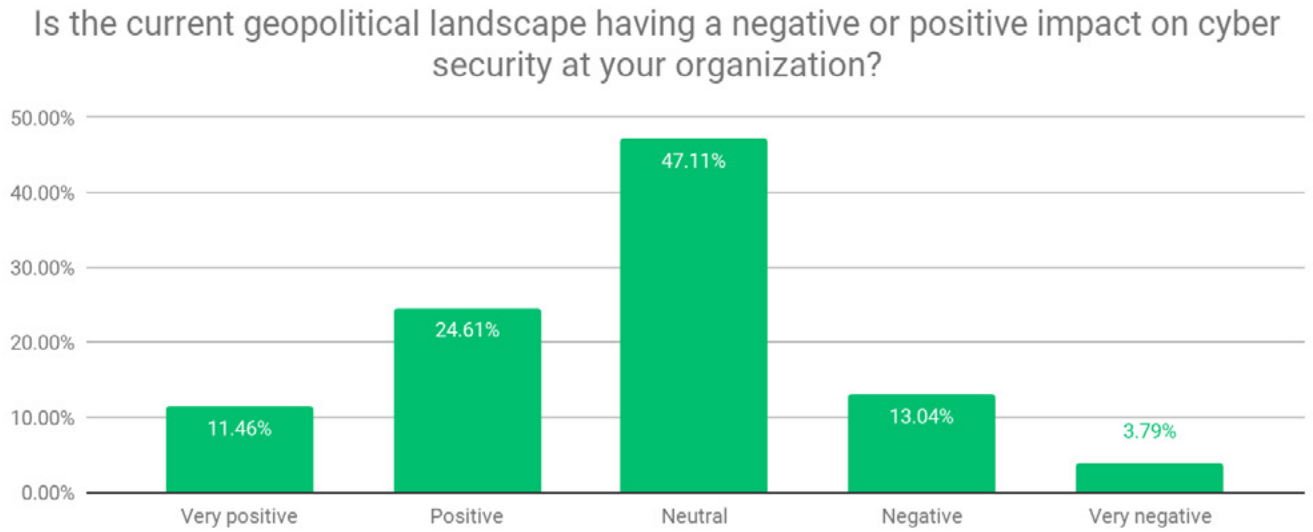
4. Geopolitics

The geopolitical arena has changed significantly in the past few years in respect to the ever-increasing technology element. For the first time ever, nation, state, and geopolitical attacks are part of mainstream media and conversation. As a result, news coverage on cyber attacks have increased and whether public infrastructure are prepared or not to withstand cyber attacks are now very much in the public eye. In fact, the majority of participants at 54% believe that the US public infrastructure is unprepared or very unprepared to defend against cyber threats.



We went further to ask what kind of impact respondeds felt that the current landscape was having on security within their organization.

The majority of respondents, at 47%, felt that there was no impact, and gave a neutral rating. The remainder were skewed more towards the current landscape having a positive or very positive impact.



Raj Samani, Chief Scientist at McAfee believes that the impact of cyber capabilities in today's landscape should not be underestimated.

"There is no question that development of offensive cyber capabilities to support national strategic imperatives are part of today's infosec landscape. Not only are capabilities being invested in, but for smaller states outsourced to even private entities."

Scot Terban, a threat researcher and self-confessed curmudgeon, echoed this sentiment:

"The notion that geopolitics and the geopolitical landscape today not affecting InfoSec would be somewhat deluded. Quite the opposite is true, and this can be measured in the amounts of change since the early days of hacking to today, quite clearly. The simple fact that nation state actors are using hacking on not only government entities, but corporations, universities, and individuals shows us all that geopolitics have become a primary motive for hacking today, as well as criminality. Also, in looking at how InfoSec has evolved, even the term is an old military/government contraction that the rest of us all have adopted in the community.

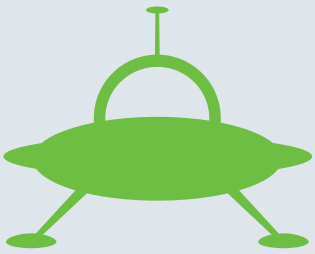
Frankly, if you pull back and look at everything we are facing today, 0day's leaked from the CIA and NSA, nation state actors leveraging hacking techniques to compromise networks and individuals for political outcomes like the 2016 elections in the US, how can one not see the connection? Every person, corporation, and entity is now confronted with the possibility of being targeted, having their personal or corporate details leaked or stolen by nation state actors or those who are paid by those actors for their own ends."

Conclusions

The cyber world is changing around us at a rapid pace. A few years ago, raising the question as to how an organization would respond to extortion attempts involving stolen data would have been scoffed at. But today, these types of cyber attacks are now top of mind for many companies. Response plans are actively being developed, and implemented (and as a result, giving CISOs another thing that could potentially disrupt their weekends).

As more companies adopt the cloud to a greater or lesser extent, cracks are beginning to appear and weaknesses in various organizations' approaches are becoming exposed. The more information we share, and not just what works well, but also what doesn't [in the cloud], and the types of security that needs to be put in place, the better off we are. When done right, the cloud can be immensely beneficial for organizations of all sizes. If the survey responses collected here are any indiciation, the industry seems to be heading in the right direction with the gap between on-premises and cloud software management closing.

Finally, it's clear that the geopolitical landscape is changing, and having a direct impact not only for enterprises, but at the national level, affecting nearly every person. For most companies, it still means they are unlikely to be impacted by a targeted attack. However, it does mean that with the trickle-down of malicious tools, techniques, and processes that many of the attack styles will become commoditized and eventually become more mainstream, much like ransom and extortion schemes that are run against companies and individuals. Therefore, it makes sense for most to look towards bolstering threat detection and response capabilities – particularly those which are continually updated with reliable threat intelligence to keep on top of the latest threats.



About AlienVault

AlienVault®, an AT&T Company, has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our phenomenal and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault's Open Threat Exchange®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.