BLACK HAT 2017 SURVEY

Ransomware & Threat Intel in Las Vegas

About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique 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. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

Table of Contents

1. Executive Summary

1.1 Introduction

It was somewhere near Mandalay Bay that the keynote began. Alex Stamos, Chief Security Officer at Facebook, walked onto the stage for the opening of the 20th annual Black Hat security conference in Las Vegas.

The huge stage, rock music accompaniment, and green laser show gave Stamos' address more of a rock concert vibe than that of a security keynote.

Empathy, community, and a focus on defense were some of the key themes highlighted by Stamos. Social media was ablaze with comments, both agreeing and disagreeing with the points he raised.

But information security is a complex field. It's easy to find oneself distracted by broad community issues or obsessing over the next zero day exploit, rather than focusing on the fundamental day-to-day issues that security practitioners face throughout the world.

To get a better sense of these fundamentals, we conducted a survey of 617 attendees at Black Hat 2017 to determine some of the biggest concerns and issues that security practitioners face on a daily basis.

The results are presented in this report with a nod to Hunter S. Thompson's *Fear and Loathing in Las Vegas*.

1.2 Key Findings

- Ransomware is the biggest concern among security professionals (42%)
- Sharing of threat intelligence continues to grow among the different channels
- 56% of respondents use open source/public threat intelligence feeds
- For 50% of respondents, the shortage of security workforce is the biggest challenge that has increased over the last year
- 64% of participants state that they are either "confident" or "very confident" in their organizations ability to detect and respond quickly to a data breach

1.3 Methodology

This report is based on the experiences of the author, a series of short discussions with security practitioners, and a survey of 617 participants at Black Hat 2017. While the analysis comes primarily from this sample, we do believe the results provide us with useful insights that are representative of the larger information security community.

Demographic data of survey respondents was not collected, and respondents were not prompted for their answers – nor was any clarification or definitions provided for the terms used.

This report was written by Javvad Malik, Security Advocate at AlienVault. Any questions about the methodology should be addressed to him at jmalik@alienvault.com.

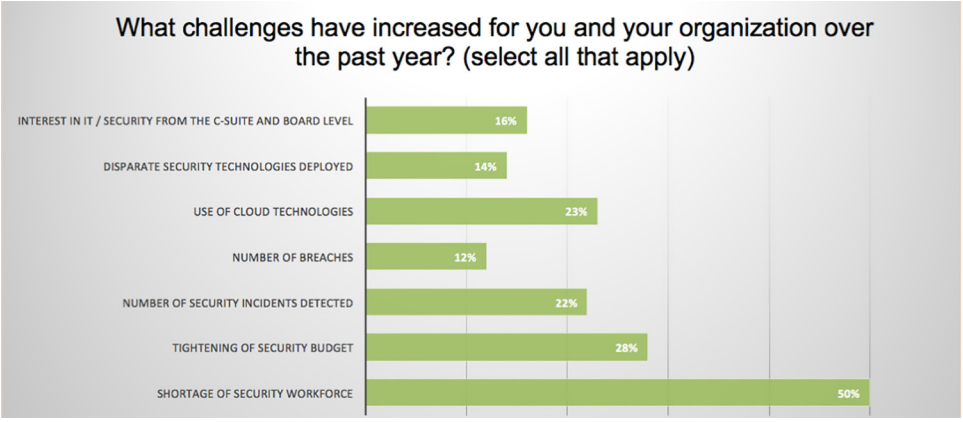
2. Security Challenges

Information security professionals can sometimes feel like Sisyphus, tasked with continuously rolling an immense boulder uphill, with no chance of respite. They often feel as if they are perpetually on the edge of a breach – struggling to find accurate ways to explain the potential risks to others who have not experienced this first-hand.

Security team leads face a plethora of challenges. Activities ranging from administrative error, nation state espionage, hacktivism, user malpractice, regulatory requirements, and everything in between, all fall under their purview – and all of these need to be addressed in a timely manner.

It's important for security teams to be on the front lines, taking the initiative to tackle challenges proactively. A team that procrastinates in prioritizing what security fires need to be put out first will inevitably have the choice made for them (and not always favorably) by circumstances.

Perhaps it is due to the enormity of the tasks faced by security professionals that nearly half of the survey participants stated that the shortage of security workforce was the biggest challenge that has increased for them over the last year.



This is an understandable concern. Whether it is educating users, writing policy, reviewing the effectiveness of controls, assessing the security requirements of new projects, responding to incidents, or implementing new technologies, every intiative needs security resources.

The second biggest concern at 28% was the tightening of security budgets.

Together, these two issues suggest a concerning trend. The lack of skills combined with a reduction of budget does not bode well for companies trying to maintain an effective level of security to not only protect their systems from common threats, but also to detect and respond to incidents in a timely manner.

Secure Because It's Amazon?

The third most pressing concern at 23% was the use of cloud technologies. The main challenges that cloud presents to security professionals are two-fold.

On one hand, there is the danger associated with shadow IT, or the use of unauthorized cloud applications. It is relatively easy for anyone to use cloud storage services such as iCloud, Google Drive, Dropbox, or any alternative to store sensitive company information. Shadow IT represents an ongoing challenge for security teams and this has increased with the rise in remote workers and the bring your own device (BYOD) trend The confluence of these two factors has decreased IT teams' visibility into all of the places where company data is stored as well as how it's being protected (or not).

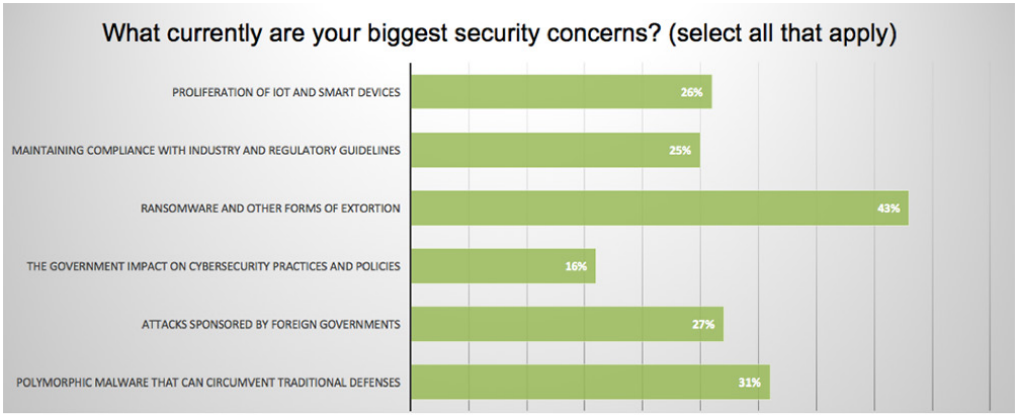
The second aspect to consider is the lack of security skills, or input from the security team, when it comes to selecting a cloud platform. Amongst many companies, “Secure Because It’s Amazon” appears to be a prevalent thought. In other words, companies often trust brand names and fail to do their own due diligence before selecting cloud service providers; they may then move sensitive workloads to the cloud without adequately securing the databases.

The concerns raised by the Black Hat survey results are well-founded. In recent months, there have been a number of incidents in which misconfigured cloud databases have resulted in the leak of millions of records – WWE, Verizon, and the personal information of Mexican voters are just three examples that made the headlines.

Moving workloads to the cloud can eliminate some forms of risks such as making sure that the latest patches are applied, or ensuring availability of systems. But the cloud also is governed by a shared responsibility model, whereby enterprises are still responsible for certain aspects of security. However, without having enough skilled staff, or the budget to invest in the right cloud monitoring tools, we could see an increase in cloud-based breaches in the future – especially amongst those organizations most affected by the issues reported by survey participants.

3. Ransomware

In today’s world of widespread threats and attacks, the only safe thing to assume is that our worst fears could come true at any moment. This is especially true when it comes to ransomware. And survey respondents agree – 43% of survey participants indicated that they were worried that their enterprise could be targeted by a ransomware attack.



Ransomware is a growing problem, affecting companies of all sizes and across all industries, and the threat is even spreading to individuals. Recent trends show that it can sometimes be as profitable for criminals to target consumers, or one-person-businesses, as it can be to target larger corporations.

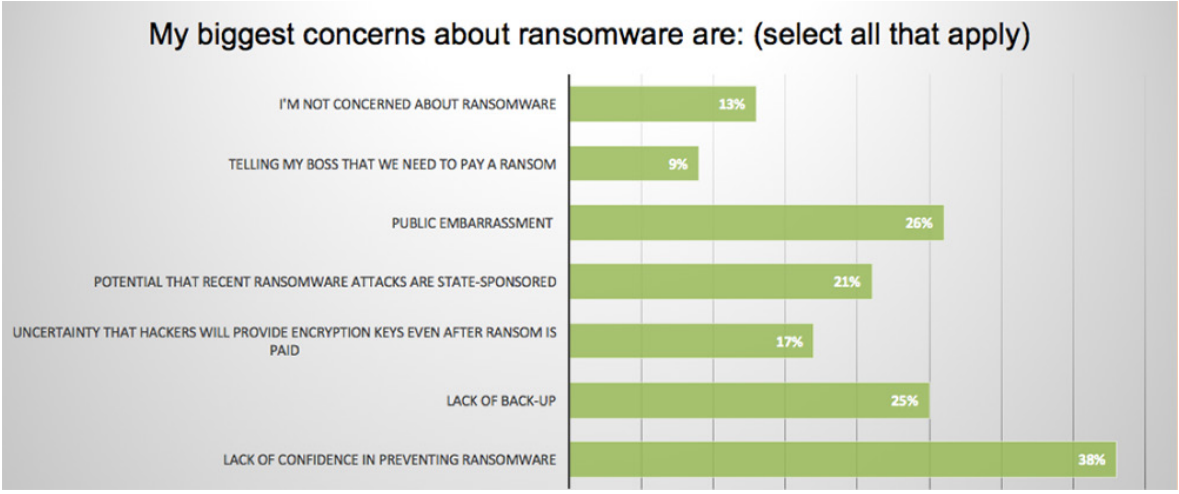
Many factors have contributed to the rise of ransomware and helped it solidify its position as a tool favored by criminals looking to make some quick money. The barriers to entry for would-be criminals have also been reduced greatly by the availability of online marketplaces and open-source ransomware. Another factor at play is the rise of ransomware-as-a-service, which offers non-technical users the chance to run their own customized ransomware campaigns with just a few clicks of the mouse.

In addition, cryptocurrency such as bitcoin allows cybercrime service providers to sell their wares easily, and enables cybercriminals to extort money from their victims effectively and from a position of relative safety behind their keyboards. This is a far cry from the days where ransom payments had to be made in person, after dark, in the basement of an abandoned carpark.

Strange Encryption and a Crisis of Confidence

For the most part, ransomware isn't intended to be 'stealthy' and neither is it generally designed to steal data. It is simply loud, in-your-face disruption, proudly displaying a message that you have been infected, and that failure to pay the demanded ransom will result in never seeing your files again.

Perhaps it is due to the loud, self-announcing nature of ransomware that public embarrassment was the second-biggest concern for respondents at 26%. This was only slightly more than the 25% of participants who cited a lack of backup as a concern.



However, by far the biggest concern with regards to ransomware, chosen by 38% of respondents, was a lack of confidence in their ability to prevent a ransomware infection.

One big question is raised by this concern: what level of confidence is there in truly being able to prevent any form of attack? The underlying narrative here is that prevention will never be enough. The wall can not be high enough and the moat will never be wide enough to prevent ALL attacks, because a patient attacker will find some way through preventative defenses, however complex. For this reason, it becomes increasingly important for organizations to focus on the threat detection and incident response aspects of security.

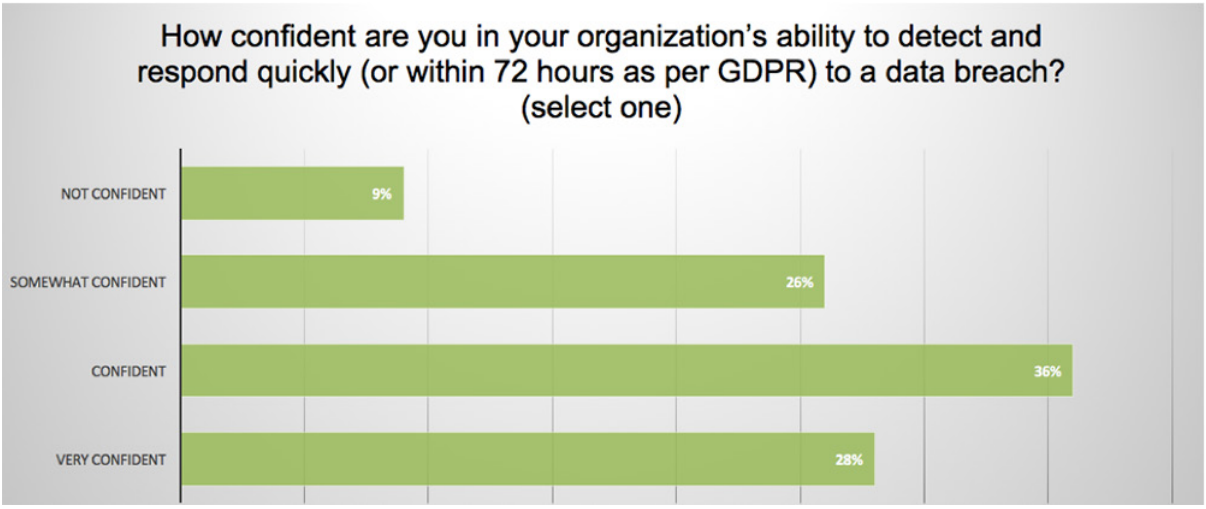
4. Detecting and Responding to Threats

One of the most basic factors in sports, and also in security, is that winning becomes a habit, and losing does too. When failure starts to feel normal in your life or your work, you don't have to go looking for trouble, because trouble finds you. This is why sitting back and relying on protective controls alone isn't sufficient.

Being able to detect threats and respond to them in a timely manner are absolutely vital components of an effective security program.

But how confident are enterprises in their ability to detect threats in a timely manner? This is a question that has plagued many over the years. The upcoming General Data Protection Regulation (GDPR) in Europe has a particular focus on breach notification, stating that whenever there is a data breach of personal information that could impact the rights and freedoms of individuals, it should be reported to the relevant supervisory authority within 72 hours of the organization becoming aware of it.

Our Black Hat survey results show significant optimism here, with 64% of participants stating they were either "confident" or "very confident" in their organizations ability to detect and respond quickly to a data breach.



As encouraging as this is, it still leaves 36% of respondents feeling only "somewhat confident" or "not confident" about being able to detect and respond to a breach in a timely manner.

Analysts Can Resolve More Incidents With The Right Music

When it comes to rapid detection and response, automation and incident response orchestration are growing trends that look to be an analyst's best friends.

Automating and orchestrating certain repetitive tasks amongst disparate products and technologies can ease the security operations burden and allow enterprises to respond to threats more quickly—and more effectively.

However, there are limits to this. Just as you would not want a machine to take over every aspect of decision-making in your life, the human element of incident response isn't going away any time soon. There are certain pieces of analysis that require human judgment, which means complete automation may not be the preferred approach in most scenarios. So, despite advancements in this area, the security challenges we discussed in section 2 will remain concerns for the forseeable future.

5. Threat Intelligence

You can turn your back on a person, but never turn your back on a good quality alert, especially when it's waving a razor-sharp hunting knife in your eye[1].

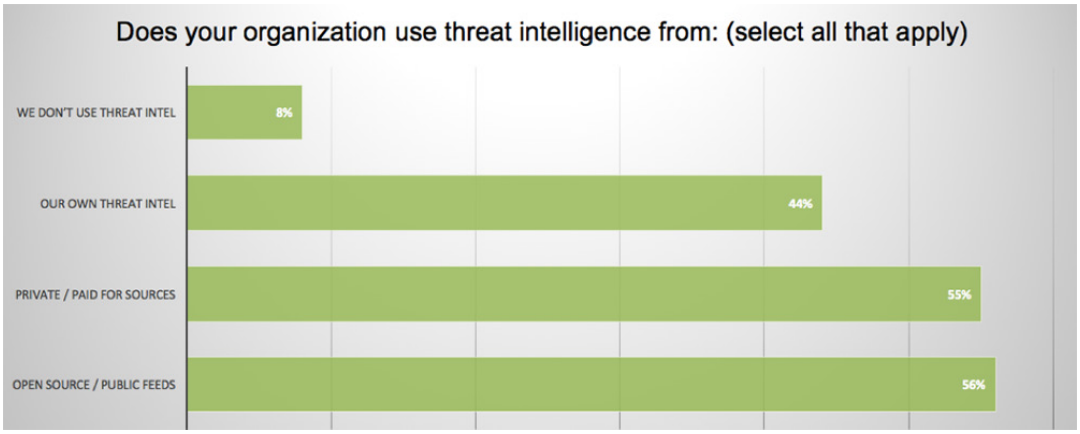
However, good quality alerts are rare in many organizations. Or to be more accurate, alerts with enough context around them to make them, dare I say it, actionable are often a rarity. This is where threat intelligence comes in.

With relevant pieces of threat intelligence accompanying it, an alert can be transformed from simply noise in the SOC, to a glittering priceless diamond[2].

But what are the most widely used sources of threat intelligence?

[1] https://www.brainyquote.com/quotes/quotes/h/huntersth153721.html

[2] https://www.brainyquote.com/quotes/quotes/h/huntersth588308.html



A majority of participants stated that they use a mixture of open source / public feeds (56%) and private / paid sources (55%) of threat intelligence.

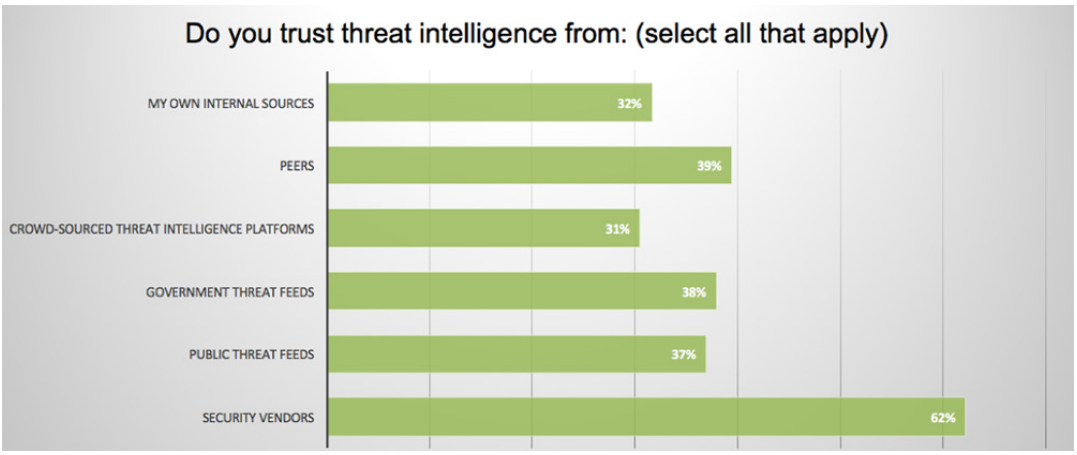
Slightly less (44%) use their own threat intelligence, likely gathered from internal sources. And only a minority at 8% stated they do not use threat intelligence at all.

Compared to last year's Black Hat survey, where we asked the same question, the percentage of companies that use their own threat intelligence has slipped from the top position to third place this year. However, overall threat intelligence is additive in nature. A company can rely on its own internal detection processes, but also complement it with both public and private threat intelligence feeds.

A Matter of Trust

Continuing our review of how trends have changed over the course of the year, we also asked what sources of threat intelligence users trust the most.

Like last year, vendors scored the highest, with 62% of participants citing that they were a trustworthy source of information. The remaining options – internal sources, peers, crowd-sourced platforms, government feeds, and public threat feeds – all scored between 30% and 39%.



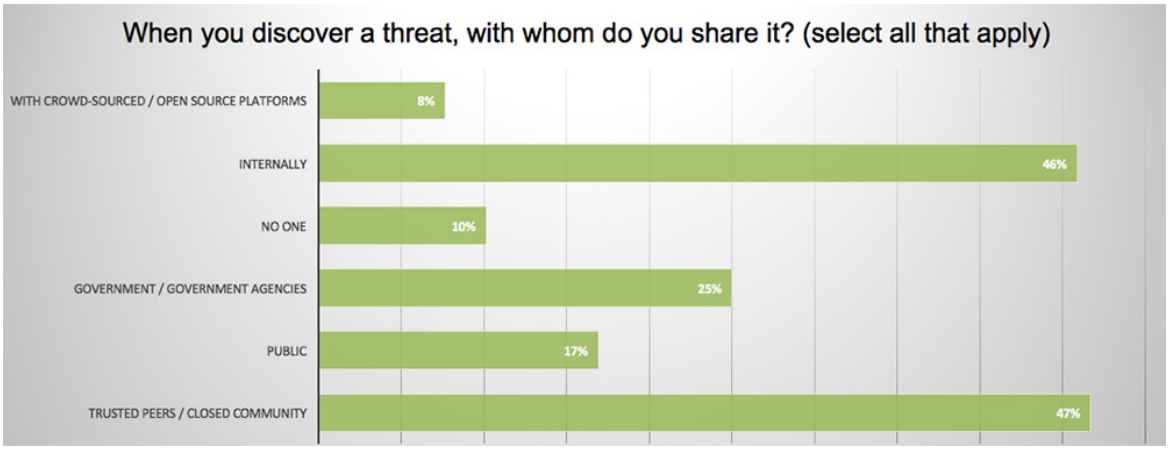
Participants weren't asked to provide a rationale for their answer, but a contributing factor could be ease-of-use. Typically when acquiring threat intelligence from a security vendor, there is an appliance, software or a portal through which the data is consumed, or integrated. This means less work for the analysts who do not have to manually sift through data to import it.

Threat Sharing, A Moral Obligation

In last year's survey, 76% of participants stated that as a security professional, they felt a moral responsibility towards the industry to share threat intelligence. But how does this translate into real-world sharing?

The highest number of respondents state that they predominantly share threat intelligence internally (46%) or within a closed or trusted peer community (47%). This is in line with surveys conducted in previous years.

Only 10% of participants state they do not share threat data with anyone, which is an encouraging sign.



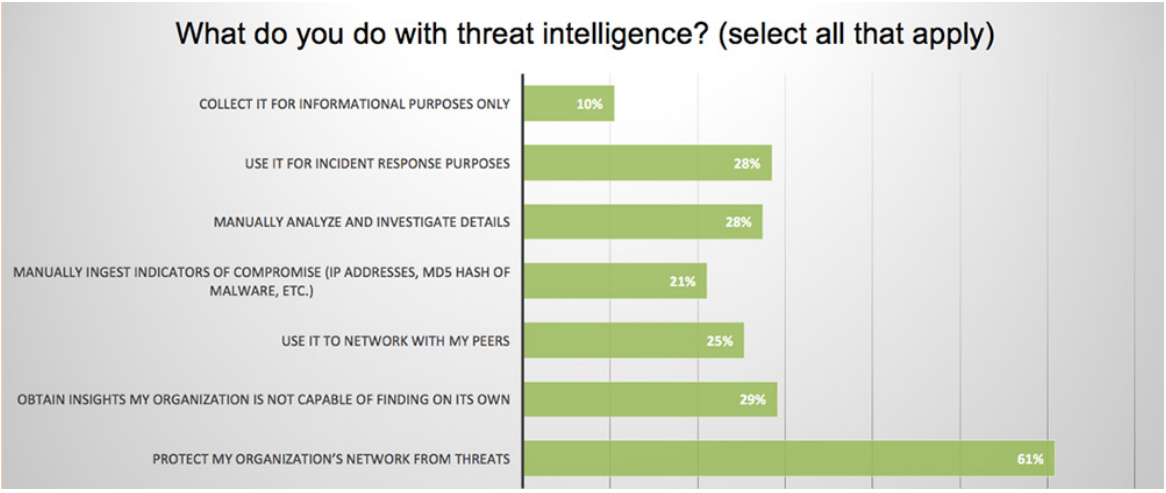
Raise The Ticket; Take The Ride

The final angle we'd like to explore from a threat intelligence perspective is how organizations are using it. It's all well and good to collate and share, but if threat intelligence doesn't have a specific use in a company's overall security program, it could end up gathering virtual dust on a server rack in a forgotten data center.

The majority of respondents, 60%, said that they use threat intelligence to protect their organization from threats.

In second place, 29% state they use threat intelligence to gain insights that their organization is not capable of finding on its own.

According to last year's survey, 40% of participants were using threat intelligence for incident response. However, this percentage dropped to 28% – and third place – in this year's survey results.



6. Tomorrow's Regulation Is Today's Reason Why

The General Data Protection Regulation (GDPR) is due to come into force in 2018 and has the potential to significantly alter the way businesses handle data. At more than 200 pages long, the regulation is possibly the most wide-ranging piece of legislation ever passed.

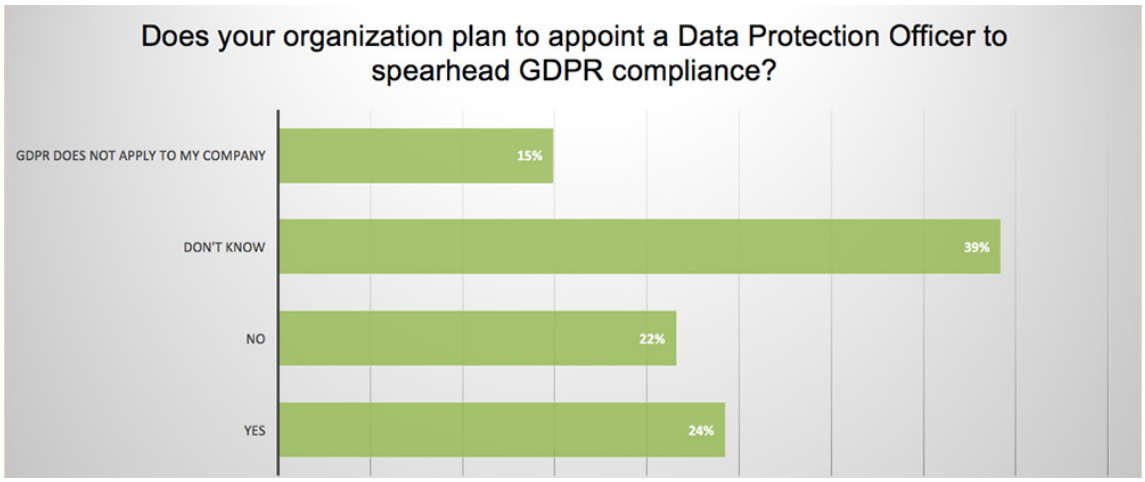
While its roots are set in Europe and its focus is on protecting European citizen and resident data, the responsibilities for security have extended significantly beyond just the data controller to also encompass companies involved as data processors. This means that US and international companies that process any data relating to EU citizens or residents will also fall under the scope of GDPR.

This is why we felt it was pertinent to ask Black Hat attendees their thoughts on the upcoming legislation.

A substantial number of respondents (46%) stated that GDPR will impact their organization.

Perhaps one of the biggest changes that GDPR will bring about is forcing companies to think about who is responsible for data protection. We asked participants if their organization was planning to appoint a data protection officer (DPO) to spearhead GDPR compliance, and a quarter of attendees stated they were planning to appoint a DPO for the sake of GDPR.

22% of participants said no, but this could also be indicative of organizations with mature security and privacy departments that already have a DPO in place. Nearly 40% of participants did not know if their organization planned to appoint a DPO.

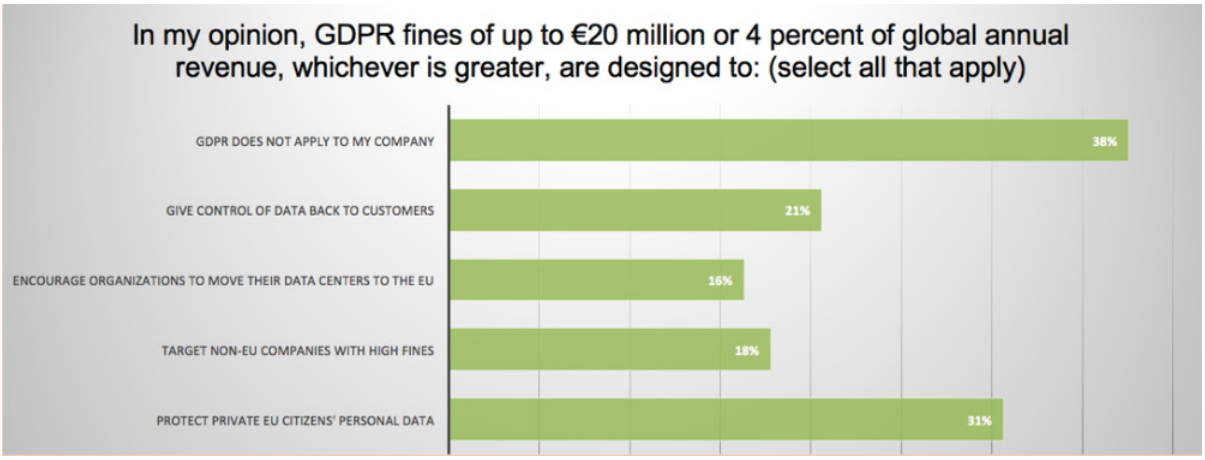


There Might Be Some Serious Fun In Regulation

Perhaps one of the biggest talking points since GDPR was published is the potential for very large fines for companies that fail to adequately protect their customer data. These could be up to €20 million, or 4% of a company's global annual revenue – whichever is greater.

But what purpose do fines actually serve? Are they simply a tool to encourage companies to move data centers into Europe? Or are they an instrument to impose high fines on non-EU companies?

Excluding participants outside the scope of GDPR, the majority (31%) stated that they believe that the fines are designed to protect private citizen data. The second largest group at 21% believe that the fines give control of data back to customers.



This is a sentiment that we can agree with. These types of fines and penalties are intended to be dissuasive. In other words, it is unlikely we will see any data regulator seek to impose anywhere near the maximum fine on any company. Rather, the mere threat of the fine should be sufficient incentive for spurring companies to take the actions required to prevent a breach from occurring in the first place.

After all, if the maximum fines are actually levied, they might end up putting some companies out of business – which wouldn't help anyone in the long run.

7. Conclusion

Can't Stop Here, It's Hack Country

The information security industry can be a weird and confusing place, despite efforts to make clear and perfect sense of it.

Ransomware doesn't look to be going anywhere soon. Rather it continues to trend upwards and grow as a threat, and companies must take appropriate steps to address this. The lack of a definitive method of preventing ransomware incidents should spur companies to focus more on detection, response, and recovery controls. For some organizations and security departments, this may require an uncomfortable shift in mindset away from the belief that all attacks can be stopped. Rather, dealing with ransomware is more an issue of risk management than it is of prevention.

Threat intelligence is a necessary component of effective security programs and we are happy to see that it continues to embed itself into the fabric of organizations. The sharing of threat data also continues to grow, as does the popularity of public and open sources of threat data.

GDPR looks like it is having a significant impact across the pond. It will be interesting to see how it unfolds and impacts service providers and other data processors going forward. The real litmus test will be when the regulation comes into effect and a breach occurs; at this point we will be able to fully gauge the true impact of GDPR on companies based outside of the EU.

As the old adage goes, "there are two types of companies; those that have been breached, and those that don't know they have been breached." The rise of ransomware has removed this ambiguity, however. It's now virtually impossible to not know when one has fallen victim to ransomware.

In some ways, dealing with security incidents is akin to being a professional gambler. All gamblers lose regularly, but they rarely discuss it in public. It's bad for the image, and nobody buys hot tips from losers.

But the game of security is about more that just winning or losing, because it does not deal in absolutes. It's all about managing risk. There is no definitive point at which companies can say: "We've achieved security." Rather, they need to accept that attacks will continue, and that breaches will occur. In fact, falling victim to an attack shouldn't be considered the end of security, but rather the point at which threat detection and response begin.

We're witnessing a change, as companies get better at detecting threats more quickly, using the right tools, threat intelligence, better processes, and skills. For this reason, looking forward, we expect threat sharing to increase for proactive threat detection purposes. Ultimately, this allows enterprises to collaboratively defend against malicious attacks with greater agility and efficiency – a strategy that will benefit not just large, well-funded enterprises, but smaller IT teams as well.

Appendix A

The Questions

Q1: What challenges have increased for you and your organization over the past year? (select all that apply)

a. Shortage of security workforce
b. Tightening of security budget
c. Number of security incidents detected
d. Number of breaches
e. Use of cloud technologies
f. Disparate security technologies deployed
g. Interest in IT / security from the C-suite and board level

Q2: What currently are your biggest security concerns? (select all that apply)

a. Polymorphic malware that can circumvent traditional defenses
b. Attacks sponsored by foreign governments
c. The government impact on cybersecurity practices and policies
d. Ransomware and other forms of extortion
e. Maintaining compliance with industry and regulatory guidelines
f. Proliferation of IoT and smart devices

Q3: My biggest concerns about ransomware are: (select all that apply)

a. Lack of confidence in preventing ransomware
b. Lack of back-up
c. Uncertainty that hackers will provide encryption keys even after ransom is paid
d. Potential that recent ransomware attacks are state-sponsored
e. Public embarrassment
f. Telling my boss that we need to pay a ransom
g. I'm not concerned about ransomware

Q4: How confident are you in your organization's ability to detect and respond quickly (or within 72 hours as per GDPR) to a data breach? (select one)

a. Very confident
b. Confident
c. Somewhat confident
d. Not confident

Q5: Does your organization use threat intelligence from: (select all that apply)

a. Open source / public feeds
b. Private / paid for sources
c. Our own threat intel
d. We don't use threat intel

Q6: When you discover a threat, with whom do you share it? (select all that apply)

a. Trusted peers / closed community
b. Public
c. Government / government agencies
d. No one
e. Internally
f. With crowd-sourced / open source platforms

Q7: Do you trust threat intelligence from: (select all that apply)

a. Security vendors
b. Public threat feeds
c. Government threat feeds
d. Crowd-sourced threat intelligence platforms
e. Peers
f. My own internal sources

Q8: What do you do with threat intelligence? (select all that apply)

a. Protect my organization's network from threats
b. Obtain insights my organization is not capable of finding on its own
c. Use it to network with my peers
d. Manually ingest indicators of compromise (IP addresses, MD5 hash of malware, etc.)
e. Manually analyze and investigate details
f. Use it for incident response purposes
g. Collect it for informational purposes only

Q9: Will GDPR impact your organization?

a. Yes
b. No

Q10: In my opinion, GDPR fines of up to €20 million or 4 percent of global annual revenue, whichever is greater, are designed to: (select all that apply)

a. Protect private EU citizens' personal data
b. Target non-EU companies with high fines
c. Encourage organizations to move their data centers to the EU
d. Give control of data usage back to customers
e. GDPR does not apply to my company

Q11: Does your organization plan to appoint a Data Protection Officer to spearhead GDPR compliance?

a. Yes
b. No
c. Don't know
d. GDPR does not apply to my company