MARKET RESEARCH

THE STATE OF CYBERSECURITY 2017 – SOUTHEAST ASIA

This report is part of Limelight Networks’ series of annual surveys that explore consumer perceptions and behaviors around online experiences.
# TABLE OF CONTENTS

State of Cybersecurity Report – Southeast Asia ............................................................... 4
Executive Summary ............................................................................................................. 5
Key Findings ....................................................................................................................... 6

**Consumers** .................................................................................................................. 6
- Smartphones are the Primary Device Used to Make Online Transactions ............................... 6
- Consumers Check the Security of a Site Before Committing to a Transaction .................... 8
- There is a Powerful Relationship Between Brand Integrity and Cyber-Attacks—When Attacks Occur, Brand Reputation Falters and Impacts Future Business ......................................................... 11
- When it Comes to Cyber-Crime, Consumers Are Most Concerned About Violations of Personal Information ......................................................... 12
- Consumers Are Extremely Concerned About the Current State of Cybersecurity, and Think Businesses Aren’t Doing Enough to Thwart the Threats ......................................................... 14

**Businesses** ................................................................................................................ 16
- The Majority of Businesses Are Actively Working to Prevent Cyber-Attacks ..................... 16
- A Significant Portion of Businesses Have Experienced Previous Attacks, and the Majority Feel Their Business is Still Vulnerable ................................................................. 18
- A Majority of Businesses Feel That a Sustained Cyber-Attack Could Have Financial and Brand Implications ................................................................. 19
- When it Comes to Deploying Cybersecurity Solutions, the Major Hurdles to Implementation Are Cost and Lack of In-House Expertise to Manage Security Solutions ................................................................. 20
- For Those Businesses Deploying Cybersecurity Solutions, a Combination of Cloud and On-Premise is Preferred ............................................................................................................... 20

Conclusions and Recommendations ................................................................................. 22
Methodology ....................................................................................................................... 23
About Limelight Networks ............................................................................................... 23
Figures

Figure 1: Which of the following devices do you use to make online transactions? (Everyone) ........................................... 6
Figure 2: Which of the following devices do you use to make online transactions? (Singapore) ................................. 7
Figure 3: Which of the following devices do you use to make online transactions? (Philippines) ................................. 7
Figure 4: Before making an online transaction, do you check to see if the site is secure? (Everyone) ...................... 8
Figure 5: Before making an online transaction, do you check to see if the site is secure? (Philippines) ...................... 8
Figure 6: Before making an online transaction, do you check to see if the site is secure? (Singapore) ...................... 9
Figure 7: Which of the following do you do to check the security of a website before making a transaction? (Everyone) .......................................................................................................................... 9
Figure 8: Which of the following do you do to check the security of a website before making a transaction? (Philippines) .......................................................................................................................... 10
Figure 9: When you hear of a company that had suffered a cyber-attack, does your opinion of that brand change? (Everyone) ......................................................................................................................... 11
Figure 10: Will you continue to make online transactions on a website that has been previously hacked? (Everyone) ........................................................................................................................................ 11
Figure 11: What is your level of concern for the following scenarios? [1] (Everyone) ......................................................... 12
Figure 12: What is your level of concern for the following scenarios? [2] (Everyone) ......................................................... 12
Figure 13: What is your level of concern for the following scenarios? [3] (Everyone) ......................................................... 13
Figure 14: How would you describe your level of concern about the state of cybersecurity now? (Everyone) .......... 14
Figure 15: How would you describe your level of concern about the state of cybersecurity now? (Philippines) .......... 14
Figure 16: How confident are you that businesses are doing enough to protect against cyber-attacks? (Everyone) ........................................................................................................................................ 15
Figure 17: Does your organization currently protect its website and applications from Distributed Denial of Service (DDoS) attacks? (Everyone) .................................................................................. 16
Figure 18: Does your organization currently protect its web applications from cyber-attacks other than DDoS? (Everyone) .................................................................................................................................. 17
Figure 19: Has your organization's website or web applications suffered a cyber-attack during the past 2 years which resulted in website downtime or loss of data? (Everyone) ........................................ 18
Figure 20: Do you think your website or web applications are vulnerable to cyber-attacks, DDoS, or being hacked? ........................................................................................................................................ 18
Figure 21: How likely would your organization suffer financial loss if your website was unavailable for 24 hours because of a DDoS attack, cyber-attack, or other hacking incident, or if your customers’ or your organization's data was stolen? (Everyone) ......................................................... 19
Figure 22: How likely would your organization's reputation suffer if your website experienced a cyber-attack? .... 19
Figure 23: If your organization has not yet deployed cyber threat protection measures, what is the primary reason? (Everyone) ........................................................................................................... 20
Figure 24: If your organization is considering deploying cybersecurity protection measures, what approach are you considering? (Everyone) .................................................................................. 20
Figure 25: Please select all the reasons you are considering cloud-based security solutions. (Everyone) .......... 21
Figure 26: Please select all reasons you are considering on-premise security solutions? (Everyone) .......... 21
STATE OF CYBERSECURITY REPORT – SOUTHEAST ASIA

The State of Cybersecurity is part of Limelight Networks’ series of annual reports that explores perceptions and behaviors around online experiences. This report combines two surveys—one examining consumers’ perceptions about the current state of cybersecurity and their concerns, and another examining what businesses are doing to address cybersecurity issues.

The first survey in this report, capturing responses from consumers in Malaysia, the Philippines, and Singapore, takes a close look at how consumers perceive the current state of cybersecurity in their online transactions. Key consumer findings include:

• Smartphones are the primary device used to make online transactions
• Consumers check the security of a site before committing to a transaction
• There is a powerful relationship between brand integrity and cyber-attacks—when attacks occur, brand reputation falters and impacts future business
• When it comes to cyber-crime, consumers are most concerned about violations of personal information
• Consumers are extremely concerned about the current state of cybersecurity and think businesses aren’t doing enough to thwart the threats

While the cyber-crime can impact a business’ reputation (and the bottom line), businesses are presented with an additional challenge—how to prevent cyber-attacks to alleviate consumer concerns. Key findings amongst business respondents include:

• The majority of businesses are actively working to prevent cyber-attacks
• A significant portion of businesses have been targets of attacks and the majority feel that their business is still vulnerable
• Most businesses feel that a sustained cyber-attack could have significant financial and brand implications
• When deploying cybersecurity solutions, the major hurdles to implementation are cost and lack of in-house expertise to manage security solutions
• For those businesses deploying cybersecurity solutions, a combination of cloud and on-premise is preferred

To help apply the insights from this report, we have included a section detailing strategies organizations can use to ensure their websites and web applications are secure while also allaying consumer fears regarding potential attacks. These include:

• Employ a multi-layered security approach
• Use a cloud-based solution
• Take advantage of a content delivery network (CDN)
• Publicize security readiness
• Be transparent about attacks
EXECUTIVE SUMMARY

Cyber-crime is on the rise. In fact, 84% of organizations surveyed in Neustar's 2017 Worldwide DDoS Attacks & Cyber Insights Research Report said they were hit with at least one Distributed Denial of Services (DDoS)\(^1\) attack in the previous 12 months, up from 73% in 2016. Plus, 86% of those attacked had to contend with more than one DDoS attack versus 82% in the previous year. DDoS attacks were often used in concert with other cyber-crime activities with a sharp rise in impact.\(^2\)

At the same time, data breaches are reaching stunning levels, with over 6 billion records exposed in the first half of 2017 alone, far exceeding the previous all-time high which was hit in 2016, reported by RiskBased Security.\(^3\)

But increasing cyber-crime hasn’t stopped consumers from continuing their online activities. Whether on smartphones, laptops, or other devices, the majority of survey respondents still complete transactions over the Internet despite the potential threats. This proclivity for e-commerce in the face of potential cyber-crime might be a result of consumer vigilance in ensuring that a website is secure (via the use of HTTPS and representing a trusted source) before completing transactions. Because when a site does get hacked, consumer confidence dips significantly with many indicating that they would not make a transaction from it in the future.

The majority of businesses responding to the survey indicated that their organization has implemented technologies to protect against DDoS and other attacks, which is especially important given that the majority of respondents also indicated that their organization’s digital presence had been attacked in the past two years, resulting in site downtime or loss of data. Perhaps that is the prime indicator in why respondents also feel that their organization’s web presence is still vulnerable to attack. In spite of that, though, many organizations still struggle with implementing the appropriate measures to prevent attacks, citing cost and a lack of in-house expertise as the primary drivers.

There is a clear correlation between consumer feelings about cyber-crime, organizations implementing the appropriate measure to thwart attacks, and the potential for loss of brand reputation and revenue because of a breach. If consumers feel safe and protected while online, they are probably more likely to shop from a specific merchant in the future.

Cyber-crime is a very complicated topic for both organizations and consumers, but if there is one thing that resonates from this report, it’s that it cannot be ignored. Both consumers and organizations must be vigilant and ready to thwart potential attacks.
KEY FINDINGS

CONSUMERS

• Smartphones are the primary device used to make online transactions.
• Consumers check the security of a site before committing to a transaction.
• There is a powerful relationship between brand integrity and cyber-attacks—when attacks occur, brand reputation falters and that impacts future business.
• When it comes to cyber-crime, consumers are most concerned about violations of personal information.
• Consumers are extremely concerned about the current state of cybersecurity and think businesses aren’t doing enough to thwart the threats.

SMARTPHONES ARE THE PRIMARY DEVICE USED TO MAKE ONLINE TRANSACTIONS

As illustrated in Figure 1, the smartphone is the leading device in Southeast Asia through which to make an online transaction while the laptop comes in second.

**Figure 1: Which of the following devices do you use to make online transactions? (Everyone)**
Interestingly enough, though, that is not necessarily the case in Singapore as illustrated in Figure 2.

As we can see in the graph above representing survey results from consumers in Singapore, laptops share the top spot with smartphones as the leading device used to make online transactions. And yet in the other countries surveyed, the smartphone is clearly the leading device.

This discrepancy between countries may represent the differences in fixed-line broadband speed. According to a recent report on Internet speeds, the Philippines has a significantly lower broadband speed than the global average (5.5 Mbps versus 7.2 Mbps) perhaps prompting the country’s inhabitants to more often use a smartphone (which, through 4G connections, might have a faster download speed) than a laptop computer.4

Figure 2: Which of the following devices do you use to make online transactions? (Singapore)

Figure 3: Which of the following devices do you use to make online transactions? (Philippines)
CONSUMERS CHECK THE SECURITY OF A SITE BEFORE COMMITTING TO A TRANSACTION

One of the issues for consumers is knowing whether a site is secure before committing to sharing highly sensitive information (such as physical addresses and credit card numbers). As illustrated in Figure 3, consumers in Southeast Asia are checking a site’s security before partaking in e-commerce or other activities.

![Bar chart showing 8.53% no and 91.47% yes for checking site security](chart1.png)

**Figure 4:** Before making an online transaction, do you check to see if the site is secure? (Everyone)

Interestingly, though, consumers in the Philippines are even more cautious (Figure 5).

![Bar chart showing 3.70% no and 96.30% yes for checking site security](chart2.png)

**Figure 5:** Before making an online transaction, do you check to see if the site is secure? (Philippines)
While those in Singapore are less concerned with the security of a site (Figure 6).

**Figure 6:** Before making an online transaction, do you check to see if the site is secure? (Singapore)

And how do consumers check the security of those sites? As illustrated in Figure 7, the primary method is by shopping only on sites the consumer already trusts.

**Figure 7:** Which of the following do you do to check the security of a website before making a transaction? (Everyone)
Interestingly, in the Philippines, consumers are considerably more likely to check with their friends to verify if the site is safe than the rest of Southeast Asia (Figure 8).

**Figure 8:** Which of the following do you do to check the security of a website before making a transaction? (Philippines)
THERE IS A POWERFUL RELATIONSHIP BETWEEN BRAND INTEGRITY AND CYBER-ATTACKS—WHEN ATTACKS OCCUR, BRAND REPUTATION FALTERS AND IMPACTS FUTURE BUSINESS

There are consequences for businesses not stopping cyber-attacks. First, as illustrated by Figure 9, is the impact to brand reputation.

![Figure 9](chart1.png)

Figure 9: When you hear of a company that had suffered a cyber-attack, does your opinion of that brand change? (Everyone)

Over 70% of consumers change their opinion of a brand after a cyber-attack. And what does this mean to the business? As shown in Figure 10, it hits the bottom line. Almost 40% of consumers will not continue to make online transactions on a website that has been previously hacked and another 40% are unsure. This clearly indicates to businesses that there is a material revenue impact to being hacked.

![Figure 10](chart2.png)

Figure 10: Will you continue to make online transactions on a website that has been previously hacked? (Everyone)
WHEN IT COMES TO CYBER-CRIME, CONSUMERS ARE MOST CONCERNED ABOUT VIOLATIONS OF PERSONAL INFORMATION

Consumers top concerns about cyber-attacks are:

- Loss of financial and/or personal information (Figure 11)
- Falling victim to an online scam (Figure 12)
- Infection of devices by malware (Figure 13)

**Figure 11:** What is your level of concern for the following scenarios? [1] (Everyone)

- **My financial and/or personal information being obtained by others without my consent:**
  - Extremely concerned: 74.48%
  - Moderately concerned: 21.98%
  - Slightly concerned: 3.07%
  - Not concerned: 0.46%

- **Falling victim to an online scam or fraud:**
  - Extremely concerned: 73.64%
  - Moderately concerned: 19.45%
  - Slightly concerned: 5.69%
  - Not concerned: 1.23%
While concerns about the loss of financial and/or personal information are slightly higher than the other two scenarios, consumers are “extremely concerned” about all three, with the majority (over 70%) indicating a significant level of anxiety.
CONSUMERS ARE EXTREMELY CONCERNED ABOUT THE CURRENT STATE OF CYBERSECURITY, AND THINK BUSINESSES AREN’T DOING ENOUGH TO THWART THE THREATS

With consumers feeling anxious about potential cyber-attack scenarios (Figures 11-13) and their reluctance to frequent websites that have been hacked before (Figure 10), it seems only natural that consumers would express a significant level of concern over the current state of cybersecurity (Figure 14).

![Graph showing consumer concerns about cybersecurity](image)

**Figure 14:** How would you describe your level of concern about the state of cybersecurity now? (Everyone)

Although as illustrated in Figure 15, consumers in the Philippines are significantly more worried about the state of cybersecurity than the rest of Southeast Asia.

![Graph showing consumer concerns in the Philippines](image)

**Figure 15:** How would you describe your level of concern about the state of cybersecurity now? (Philippines)

As demonstrated in Figure 14, almost 60% of consumers are “extremely concerned” about cybersecurity today (whereas almost 74% of consumers in the Philippines are “extremely concerned”), which is understandable given many of the high-profile attacks happening around the globe. One would think that given this situation, businesses would be more apt to implement cybersecurity measures to ensure the trustworthiness of their websites and online applications. But consumers don’t quite believe that is happening.
Figure 16: How confident are you that businesses are doing enough to protect against cyber-attacks? (Everyone)

Only 21% of consumers feel “extremely confident” that businesses are doing enough to protect them against cyber-crime. It’s possible that such a business response to cyber-attacks could significantly impact consumer trust of an online property which, in turn, might have a bearing on brand reputation and long-term transactions.
KEY FINDINGS

BUSINESSES

• The majority of businesses are actively working to prevent cyber-attacks.

• A significant portion of businesses have been targets of attacks and the majority feel that their business is still vulnerable.

• A majority of businesses feel that a sustained cyber-attack could have significant financial and brand implications.

• When deploying cybersecurity solutions, the major hurdles to implementation are cost and lack of in-house expertise to manage security solutions.

• For those businesses deploying cybersecurity solutions, a combination of cloud and on-premise is preferred.

THE MAJORITY OF BUSINESSES ARE ACTIVELY WORKING TO PREVENT CYBER-ATTACKS

As indicated in the consumer section of this report, people are not feeling particularly confident that organizations are doing enough to thwart cyber-crime and other electronic attacks. As illustrated in Figures 17 and 18, organizations are, in fact, actively protecting website and applications from DDoS and other types of cyber-crimes.

**Figure 17:** Does your organization currently protect its website and applications from Distributed Denial of Service (DDoS) attacks? (Everyone)
Figure 18: Does your organization currently protect its web applications from cyber-attacks other than DDoS? (Everyone)

Despite this focus on implementing cybersecurity protections, consumers still feel that enough isn’t being done (Figure 16). Organizations may be able to offset those concerns by being more public in their pronouncements about cybersecurity readiness. For example, companies could put icons and other imagery on the site that indicate the use of different technologies being employed to thwart cyber-attacks.
A SIGNIFICANT PORTION OF BUSINESSES HAVE EXPERIENCED ATTACKS, AND THE MAJORITY FEEL THEIR BUSINESS IS STILL VULNERABLE

Despite the readiness indicated in Figures 17 and 18, many respondents report that their organizations have suffered a cyber-attack (Figure 19).

![Figure 19: Has your organization's website or web applications suffered a cyber-attack during the past 2 years which resulted in website downtime or loss of data? (Everyone)](image)

![Figure 20: Do you think your website or web applications are vulnerable to cyber-attacks, DDoS, or being hacked?](image)

What’s more, though, as Figure 20 illustrates, the majority of companies who haven’t suffered a cyber-attack in the last two years feel their organization’s digital presence is still vulnerable to possible attack.
A MAJORITY OF BUSINESSES FEEL THAT A SUSTAINED CYBER-ATTACK COULD HAVE FINANCIAL AND BRAND IMPLICATIONS

Just as many respondents still felt their website or web application was vulnerable to cyber-attack, most (over 70%) also feel that such an attack would have a financial impact (Figure 21).

![Figure 21: How likely would your organization suffer financial loss if your website was unavailable for 24 hours because of a DDoS attack, cyber-attack, or other hacking incident, or if your customers’ or your organization’s data was stolen? (Everyone)](chart)

But the impact of an attack isn’t just financial. As consumers indicated (Figure 9), brand reputation can suffer in the event of an attack as well, a sentiment that is mirrored by the business respondents in Figure 22. Over 75% of respondents indicated a likelihood of brand reputation impact if a cyber-attack were to happen to their website or web application.

![Figure 22: How likely would your organization’s reputation suffer if your website experienced a cyber-attack? (Everyone)](chart)
WHEN IT COMES TO DEPLOYING CYBERSECURITY SOLUTIONS, THE MAJOR HURDLES TO IMPLEMENTATION ARE COST AND LACK OF IN-HOUSE EXPERTISE TO MANAGE SECURITY SOLUTIONS

Putting the feelings about vulnerability aside, and the potential for negative financial/brand impact in the event of a cyber-attack, what are businesses doing about implementation? It appears, as depicted in Figure 23, that the biggest hurdle for implementation (amongst those organizations that have yet to deploy a solution) is the cost of the cybersecurity technology, followed closely by a lack of security expertise.

![Figure 23: If your organization has not yet deployed cyber threat protection measures, what is the primary reason? (Everyone)](image)

FOR THOSE BUSINESSES DEPLOYING CYBERSECURITY SOLUTIONS, A COMBINATION OF CLOUD AND ON-PREMISE IS PREFERRED

Digging into the details of implementation, the majority of respondents favored a combination of cloud-based and on-premise solutions (Figure 24).

![Figure 24: If your organization is considering deploying cybersecurity protection measures, what approach are you considering? (Everyone)](image)
Cost effectiveness is the primary reason respondents are considering cloud-based solutions, followed closely by the broad defensive surface such solutions provide. (Figure 25).

![Figure 25: Please select all the reasons you are considering cloud-based security solutions. (Everyone)](image)

Respondents cited optimization as the primary reason to select an on-premise solutions, with the ability to maintain greater control as a secondary factor. (Figure 26).

![Figure 26: Please select all reasons you are considering on-premise security solutions? (Everyone)](image)

It would seem that organizations are looking for the best of both worlds. By combining cloud and on-premise, they can achieve a more cost-effective, yet ultimately configurable, solution that also leverages existing expenditures (i.e., in-house expertise).
CONCLUSIONS AND RECOMMENDATIONS

Securing websites and web applications will always be a challenge given the constant evolution of attack methodologies, but there are strategies organizations can apply to protect their business and reassure consumers. These strategies include:

- Employ a multi-layered security approach
- Use a cloud-based solution
- Take advantage of a CDN
- Publicize security readiness
- Be transparent about attacks

EMPLOY A MULTI-LAYERED SECURITY APPROACH
Cybersecurity isn’t a “one-size-fits-all” approach. There isn’t a single solution that prevents all kinds of attacks. For example, on-premise solutions are great for Layer 7 attacks but may not be good against volumetric attacks like DDoS. It’s critical that organizations look at their entire website or web application architecture and develop an approach that layers cloud and on-premise technologies into a “cybersecurity stack” which can protect consumers from a variety of different vectors.

USE A CLOUD-BASED SOLUTION
Although on-premise cybersecurity solutions represent some of the best technology, ultimately, they often aren’t scalable enough (by themselves) to handle a large attack against a distributed website or web application. Cloud solutions, on the other hand, are built to scale. What’s more, they don’t require software updates or upgrades to maintain effectiveness against the latest cyber-attacks. Finally, as indicated in the data from our report, cloud solutions are more cost effective than on-premise technologies.

TAKE ADVANTAGE OF A CDN
In addition to a dedicated cybersecurity solution, it’s critical that organizations employ a CDN which can buffer volumetric attacks. Not only can a CDN mitigate DDoS and other high-volume cyber-attacks, but employing a CDN for website/web application delivery and performance can have a significantly positive impact on the end-user experience by improve the speed and quality of content delivery.

PUBLICIZE SECURITY READINESS
Organizations need to do a better job of letting consumers know that they are taking steps to guard against cybersecurity threats. That may be as simple as promoting specific logos of cybersecurity solution vendor products on the website or web application. Regardless of the method, organizations need to assure consumers that they are protected against potential threats.

BE TRANSPARENT ABOUT ATTACKS
Attacks are going to happen. Unfortunately, many organizations that come under cyber-attack don’t let consumers know, leaving them to find out through news outlets. This can seriously undermine trust and brand reputation. Rather than waiting until consumers find out on their own, organizations that have sustained cyber-attacks or other intrusions should proactively let their visitors or users know what has happened and what the organization is doing to prevent possible future events.
METHODOLOGY

This survey was fielded by a third-party company with access to domestic Malaysia, Philippines, and Singapore respondents through consumer panels. The survey includes respondents only in those three countries.

The consumer portion features responses from 1,301 respondents while the business portion features responses from 316 respondents. Business respondents were filtered based on their contribution to their organizations cybersecurity readiness.

ABOUT LIMELIGHT NETWORKS

Limelight Networks Inc., (NASDAQ: LLNW), a global leader in digital content delivery, empowers customers to better engage online audiences by enabling them to securely manage and globally deliver digital content, on any device. The company’s award-winning Limelight Orchestrate™ platform includes an integrated suite of content delivery technology and services that helps organizations secure digital content, deliver exceptional multi-screen experiences, improve brand awareness, drive revenue, and enhance customer relationships — all while reducing costs.

Limelight Cloud Security Services use the Orchestrate Platform’s global reach to provide a layered defense against malicious website attacks and unauthorized content access. These services include:

- Proactive DDoS protection and mitigation
- Web Application Firewall (WAF) services to detect and block threats
- Security of content in transit against theft by one of the world’s largest SSL footprints
- Multiple access control methods to protect digital assets without adding latency to the delivery experiences

For more information, please visit www.limelight.com, read our blog, and follow us on Twitter, Facebook and LinkedIn.

---

1 DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. http://www.webopedia.com/TERM/D/DDoS_attack.html
5 This might be a result of a number of high-profile attacks in which numerous government websites have been defaced by hacktivist groups. In fact, the Philippines are ranked 33rd out of 230 countries in a 2015 Kaspersky report ranking each country’s proneness to cyber-attack. https://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines
6 Note: this question is a follow-on to the question captured in Figure 16 and represents respondents who answered “No” or “I don’t know.”