THE TRUST FACTOR

Cybersecurity's Role in Sustaining Business Momentum

Executive Summary

In 2018, the stakes for cyberattacks were higher than ever. Attention-grabbing data security incidents continued to make news, including the largest distributed denial-of-service attack ever recorded at 1.7Tbps.1 In the European Union, the General Data Protection Regulation (GDPR) went into effect on 25 May 2018, imposing strict new rules on how personally identifiable information (PII) is collected, processed and controlled. In addition, cryptominers infiltrated networks looking for a quick score.

We've entered a "post-trust" era when organisations and individuals are increasingly wary of accepting promises of security at face value. Every time consumers interact with a brand, they make a judgment about whether they trust a company enough to share their PII. Successful cyberattacks break the trust that companies have worked hard to establish between their brands and customers. Ramifications are no longer the sole responsibility of security professionals; C-suite executives are accountable as well.

To provide insights into the complex challenges faced by organisations as they fight to protect their brands, Radware produces an annual Global Application & Network Security Report. This eighth annual version of the report combines Radware's organic research, real attack data and analyses of developing trends and technologies with the findings from a global industry survey.

The report highlights the business and technology impacts of cybersecurity, including:

- Lessons learned from recent attacks
- The true costs of cyberattacks, both quantitative and qualitative
- An overview of the network and application threat landscape
- Insights into vulnerabilities of emerging technologies
- Predictions for 2019

KEY FINDINGS

Balancing the Cost vs. Risk Calculation

Protecting against cyberattacks requires a significant investment that falls on the operating expenses side of the balance sheet. By nature, organisations are always looking for ways to conserve funds. But how much is enough when you factor in the risk of cyberattacks penetrating defences and impacting businesses?

Consider these revealing insights from Radware's 2018-2019 global industry survey:

- In just one year, the initial costs attributable to cyberattacks increased 52% to £0.8 million
- Organisations that modelled overall costs of cyberattacks to their firms estimated the amount at nearly double versus companies that did not model costs
- Two in five companies reported negative customer experiences and reputation loss following a successful attack
- Ninety-three percent of respondents experienced a cyberattack in the past 12 months; only seven percent claimed not to have experienced an attack
- Cyberattacks were a weekly occurrence for one-third of organisations
- The primary impact of cyberattacks was service disruption, reported by almost half of respondents. Attacks resulting in a complete or partial service disruption grew by 15% and hurt productivity
- Cyber-ransom continued to be the leading motivation of hackers and was the reason for 51% of the attacks

Emerging Attack Vectors

Attackers employ efficient techniques to cause denial of service, such as bursts, amplification, encryption or internet of things (IoT) botnets, and target the application layer to cause more harm.

- Application-layer attacks caused the most damage. Two-thirds of respondents experienced application attacks. One-third foresee application vulnerabilities being a big concern in 2019, especially in cloud environments. More than half made changes and updated applications monthly, while the rest made updates more frequently, driving the need for automated security.
- Cyberassaults resulting in a complete outage or service disruption grew by 15%, and one in six organisations reported having suffered a 1Tbps attack.
- Hackers found new tactics to bring down networks and data centres: HTTPS Floods grew 20%, DNS and Burst attacks both grew 15% and bot attacks grew 10%.
- A third of companies reported suffering attacks for which they could not identify the motive.

Preparing for What's Next

Businesses indicate that they understand the seriousness of the changing threat landscape and are taking steps to protect their digital assets, but the severity of security threats weighs heavy.

- Nearly half felt ill-prepared to defend against all types of cyberattacks, despite having security solutions in place.
- Eighty-six percent of businesses explored machine-learning and artificial intelligence (AI) solutions in the past 12 months. Almost half said that quicker response times to cyberattacks were the motivation. Radware saw a 44% growth in those conducting business over blockchains.
- Companies continued to diversify network operations across multiple cloud providers. Two in five organisations use hybrid cybersecurity solutions that combine on-premise and cloud-based protection.
- Forty-nine percent of organisations in EMEA said that they were not well prepared for GDPR.

The Only Option Is Success

The cost of cyberattacks is simply too great to not succeed in mitigating every threat, every time. Customer trust is obliterated in moments, and the impact is significant on brand reputation and costs to win back business. The GDPR and other government regulations have the capacity to bankrupt businesses that do not comply.

It is critical for organisations to incorporate cybersecurity into their long-term growth plans. Securing digital assets can no longer be delegated solely to the IT department. Rather, security planning needs to be infused into new product and service offerings, security, development plans and new business initiatives. The CEO and executive team need to lead the way in setting the tone and investing in securing their customers' experience.

C-Suite Perspective

CEOs Are the New Trust Officers

Cybersecurity is becoming a very personal topic for executives trusted to lead companies at the highest level. To build and maintain solid relationships with customers, CEOs must take on an additional role as "chief security officer". When the years of curating a brand strategy can be obliterated with one cyberattack, assigning security strategy to the chief information security officer (CISO) is no longer enough. There is too much at stake.

Consider the fates of CEOs at companies with high-profile breaches such as Equifax, Yahoo, Moller-Maersk and Anthem Healthcare. All of the work that the organisations put into building their brands' value evaporated the moment customers lost trust as a result of the attacks. Before long, the CEOs of most of these companies were "pursuing other interests".

To ensure cybersecurity is an integral part of the companies' business models, CEOs need to verify efforts and fund protective measures. CEOs who delegate security strategy without oversight do so at their own peril.