CYBERCRIME & THE INTERNET OF THREATS 2017

Whitepaper

www.juniperresearch.com

JUNIPER RESEARCH

1.1 Introduction

As more and more business infrastructure moves online, so do those wishing to destroy or defraud that infrastructure. Cybercrime is a growing threat to corporations and consumers, who are increasingly using online methods to run their businesses and lives. With the advent of mobile computing and an expected 46 trillion connected devices in use by 2021, this will become more and more common.

This research presents the latest observable trends in cybercrime, as well as indicating the potential global cost of malicious software use. It will discuss specific threats to financial and device-based businesses, as well as providing analyses of the current and future trends in cybercriminal activity, alongside general advice on how to prevent and/or minimise the impact of cybercrime.

1.2 Cybercrime Trends

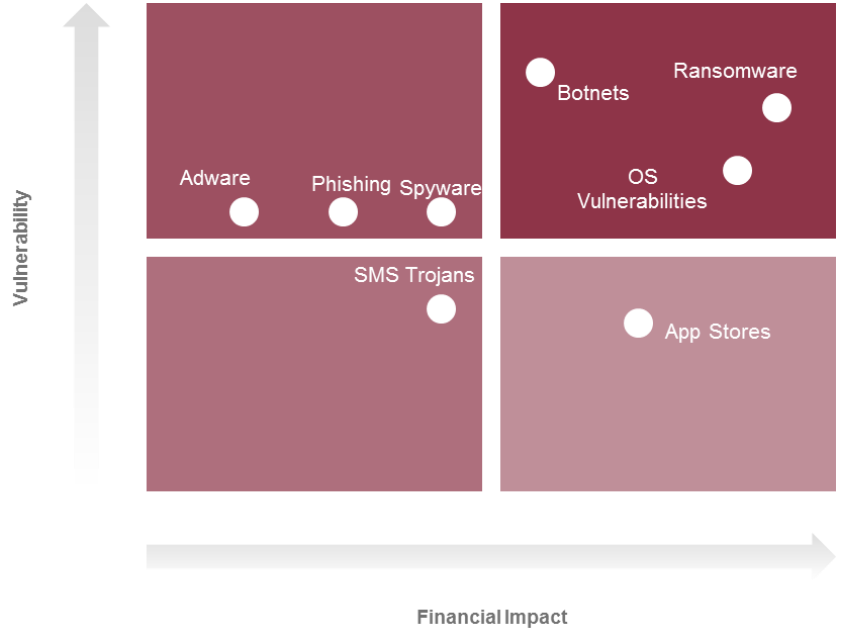
1.2.1 Social Engineering is Still Key

While the precise route of cybercriminals accessing computer systems will evolve depending on the precise nature of the OSs (operating systems), network architecture and the motivations of the cybercriminals, the basic route often remains the same; duping a user into opening the door. Social engineering remains a vital component of many cybercrime efforts.

1.2.2 Ransomware Comes of Age

The use of ransomware accelerated hugely during 2015 and 2016, with multiple cybersecurity organisations registering large increases in the use of this kind of attack. Several prevalent new variants of the software have also come into use. With an expansion of the IoT (Internet of Things) and a glut of data that is only of direct value to particular users, this is only likely to increase in the future.

Figure 1: Juniper Device Cybercrime Threat Landscape Forecast



Source: Juniper Research

This trend means that to stay current, consumer cybersecurity needs to focus away from antivirus and move to other forms of cybercrime prevention. This is particularly true for consumers sharing data between several IoT devices, and in essence forming their own device networks, a trend which will increase in the years ahead with the rise of smart home devices.

1.2.3 DoS is a Changing Threat & Distraction

Multiple cybersecurity players state that DoS (Denial of Service) attacks are frequently a mask for something else an attacker is doing. With the development of botnets that can change parts of the net's target and function mid-attack, this is becoming more prevalent.

DDoS (Distributed Denial of Service) attacks are also now frequently attacking the root DNS services of a network, rather than the application layer. This amplifies the effect of the attacks by taking down the structure supporting the services, rather than just the services themselves. It also creates a string of legitimate traffic from retry requests from other servers, amplifying the effect. By targeting the DNS layer, the attacker shifts the burden of protection from businesses to their network partners to prevent DDoS attacks.

1.3 Cybersecurity Market Trends

This section discusses trends for the following cybersecurity categories:

- Access & Identity Management – products that monitor and control account access and privileges that attach to those accounts.
- Cloud Security – a security service that provides visibility and control over cloud data traffic flow and/or cloud access, or provides backup and/or recovery services for cloud data loss.
- Network & Endpoint Security – endpoint cybersecurity products protect the access points to a network, such as PCs, smartphones, servers and data centres. Most consumer cybersecurity products are effectively forms of endpoint security, connecting to the Internet rather than a corporate network. Network security is an extension of this, monitoring and containing network traffic, as well as potentially programs that operate on network infrastructure (depending on the particular company).
- Threat Intelligence – the provision of knowledge about existing or potential threats to an organisation's network and devices. Such products may, but do not necessarily, provide advice and guidance to inform threat response.

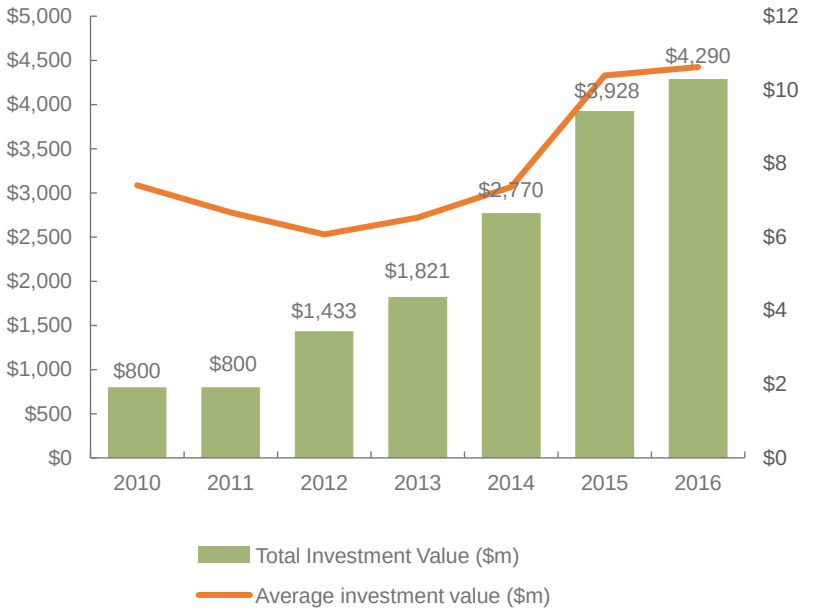
Within each of these categories there exist multiple kinds of security provision, but many vendors focus only on a single area of cybersecurity. This creates a vast array of cybersecurity providers producing a situation that is difficult to manage for end users, resulting in a situation where threats may be missed.

We therefore believe that the most successful cybersecurity businesses, regardless of their area of focus, will be those who partner with other entities to combine the different elements of cybersecurity into an integrated system.

Investments are moving away from traditional endpoint, web and mobile security towards program-level and network security. The array of

different solutions on offer from many players is also a benefit for MSSPs (managed security service providers), as many companies, particularly SMEs (Small & Medium Enterprises), do not have the resources to monitor cybersecurity threats themselves so are happy to outsource the capability to an external provider.

Figure 2: Total Disclosed Cybersecurity Investment Value per annum ($m) & Average Investment Value ($m), 2010-2016



Source: Juniper Research

1.3.1 Access & Identity Management

At the forefront of merging compliance and cybersecurity provision, access and identity management tools are becoming increasingly common cybersecurity tools for enterprise. However, it is still not a standard tool for many, particularly SMEs.

With the notion of online access and identity becoming increasingly fluid thanks to cloud storage and computing, access to the right portions of cloud data and how that access is handled once it exists is becoming a vital part of that offering. Cloud security providers are now beginning to include access management tools with their main cloud-focused offerings.

1.3.2 Cloud Security

The availability of cloud services to both consumers and businesses means that access to cloud services can increasingly come from any location. As a result, cloud security providers have shifted from a model of perimeter defence between a trusted zone and an untrusted zone, but, mirroring the moves of network security more broadly, have assumed an environment where any form of traffic is potentially unsafe. The increasing levels of encrypted traffic beginning to pass through the Internet, are making this a necessity; much encrypted data cannot be examined by any form of preventative measure until it is delivered, and therefore cannot be verified

1.3.3 Network & Endpoint Security

Endpoint security, in the form of antivirus and firewalls, has been the predominant form of cybersecurity for many years. Consumer endpoint

security and antivirus have long been freemium offerings and are typically licensed per endpoint for the enterprise, although a different model (or at least different pricing scales) is likely to be necessary for endpoint security provision for the IoT.

It is still by far the most common form of cybersecurity used by consumers and required by CISOs (Chief Information Security Officers), despite its typically incomplete protection for businesses.

As a result of this, endpoint security can, and should, become the beginning of a conversation about broader cybersecurity with CISOs and other stakeholders. However, this needs to be treated as something other than simply upselling; the additional protections offered need to be made clear to the end user, as well as being integrated with the endpoint offerings for ease of use.

1.3.4 Threat Intelligence

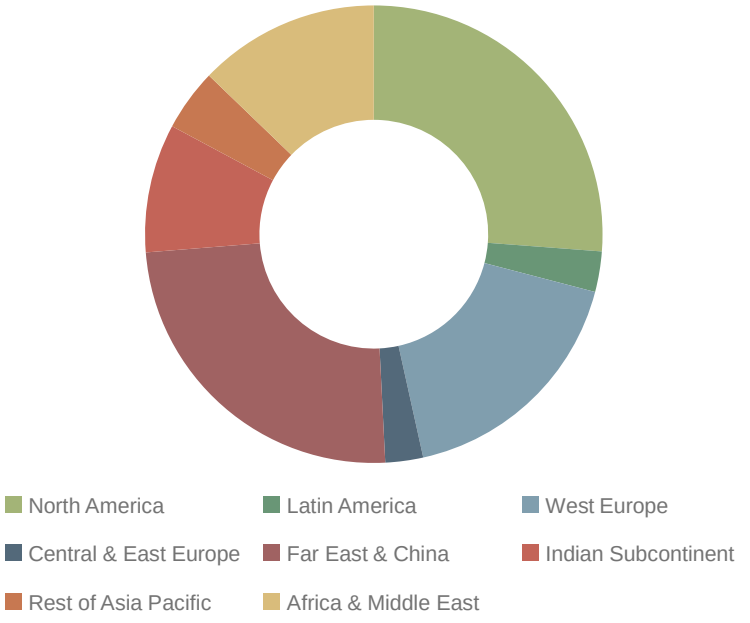
Threat intelligence vendors are increasingly shifting to ways of eliminating false positives and information overload for information security professionals, moving to AI (Artificial Intelligence) and automation of much of the threat analysis process.

Due to the ability to use automation and machine learning capabilities in tandem for cybersecurity, threat intelligence is likely to cease being a discrete business type in the future. Several endpoint security providers are already positioning their offerings as incorporating threat intelligence, and threat intelligence vendors can offer real-time network and endpoint protection as a simple extension their core intelligence offerings. Specialised diagnostics tools may still exist as part of the software used by MSSPs, but this will soon become another element of endpoint protection for business customers.

1.4 Cybersecurity Market Forecast: 2022

We estimate that the annual spend for enterprise cybersecurity products will reach almost $135 billion by 2022, a CAGR (Compound Annual Growth Rate) of 7.5% over the forecast period.

Figure 3: Global Cybersecurity Spend in 2022: $135 billion



Source: Juniper Research

- Note that this forecast includes all dedicated cybersecurity hardware and software purchases, as well as the services revenues of MSSPs. However, this does not include wages for in-house cybersecurity staff used by an organisation.
- The amount that large businesses spend on cybersecurity will increase significantly, growing at a CAGR of 7.5%, as both the necessity of contracts for AI-based protection and an expansion of endpoint coverage required for the IoT necessitates higher spending. However, the cultural change required in many organisations to invest significantly higher funding is only happening slowly. Anticipated budgetary increases will remain in the single figures per annum for the foreseeable future.

Order the Full Research

The new study, The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022, provides need-to-know information on the state of cybersecurity legislation, market trends and how the key players in cybersecurity are reacting to these developments.

Key Features

- **Threat Landscape:** Learn what the main cyberthreats are facing enterprises and consumers in 2017 and beyond.
- **Juniper Leaderboard & Vendor Analysis:** Key player capability and capacity assessment for 20 enterprise cybersecurity providers, split by Network & Endpoint Security and Cloud & IoT Cybersecurity.
- **Market Dynamics:** Understand the current market landscape, future developments and funding opportunities for the cybersecurity market.
- **Interviews:** Gain unique insight from 7 leading players, including Barracuda Networks, Cylance, FireMon, Giesecke + Devrient , Herjavec Group, SAS, Synack.

What's in this Research?

- **Key Trends & the Future Direction of Cybercrime** : Breakdown of threats and market developments by segment.
- **Legislation & Funding Analysis**: Recent and future state funding, cybersecurity legislation and an assessment of the impact of these government actions, alongside trends in the cybersecurity investment space.
- **Vendor Analysis & Leaderboards:** Capability and product assessment of 12 players in Network & Endpoint security and 12 Cloud and IoT cybersecurity providers.
- **Market Sizing & Forecasts**: Regional 5 year forecasts for the cost of data breaches and the anticipated levels of cybersecurity spend. The study includes breakdowns of the cost of data breaches, alongside average breach cost, size, number of breaches and level of breach reporting, along with cybersecurity spend levels for small, medium and large businesses.
- **Interactive Forecast Excel** – Highly granular dataset comprising more than 1,600 data points, allied to regional and sector analysis tools (Interactive XL).

Publications Details

Publication date: February 2017

Author: James Moar

Contact Jon King, Sales & Marketing Manager, for more information:
Jon.King@juniperresearch.com

Juniper Research Ltd, Church Cottage House, Church Square, Basingstoke, Hampshire RG21 7QW UK

Tel: UK: +44 (0)1256 830002/475656 USA: +1 408 716 5483 (International answering service) Fax: +44(0)1256 830093

http://www.juniperresearch.com