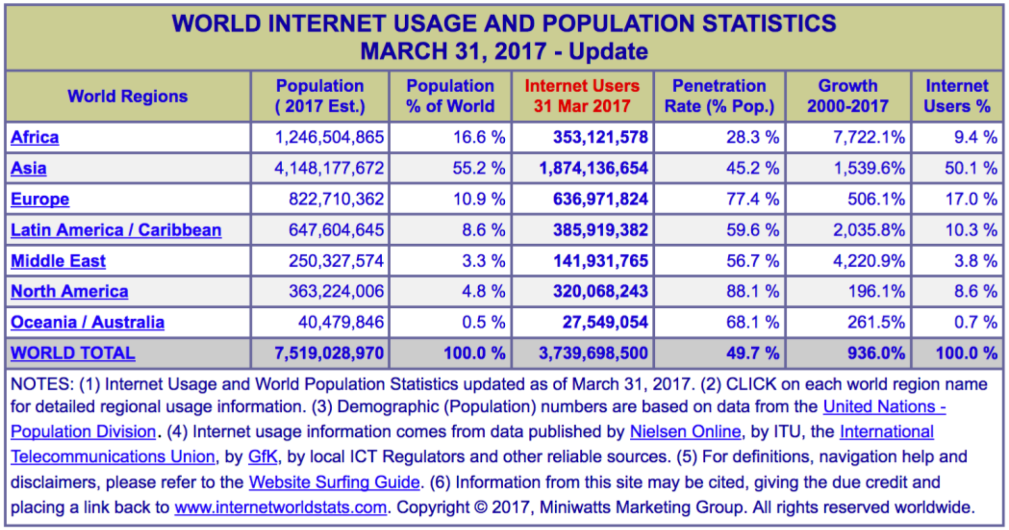
Service Provider View of Cyber Security

July 2017

LIBERTY GLOBAL

Quick Stats

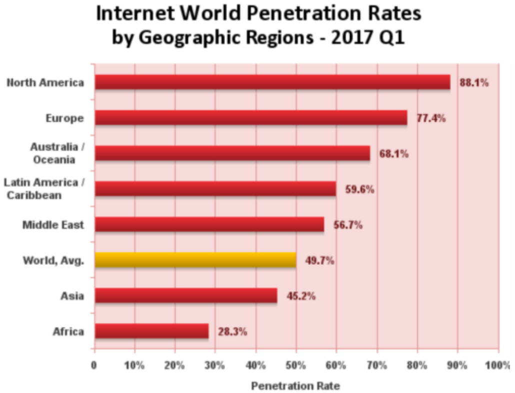
Caribbean and LatAm: 3rd largest population of Internet Users



WORLD INTERNET USAGE AND POPULATION STATISTICS
MARCH 31, 2017 - Update

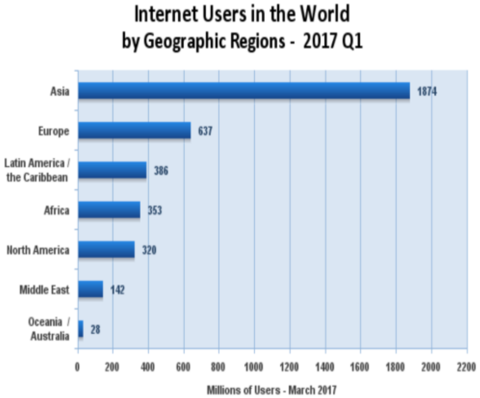
World Regions	Population (2017 Est.)	Population % of World	Internet Users 31 Mar 2017	Penetration Rate (% Pop.)	Growth 2000-2017	Internet Users %
Africa	1,246,504,865	16.6 %	**353,121,578**	28.3 %	7,722.1%	9.4 %
Asia	4,148,177,672	55.2 %	**1,874,136,654**	45.2 %	1,539.6%	50.1 %
Europe	822,710,362	10.9 %	**636,971,824**	77.4 %	506.1%	17.0 %
Latin America / Caribbean	647,604,645	8.6 %	**385,919,382**	59.6 %	2,035.8%	10.3 %
Middle East	250,327,574	3.3 %	**141,931,765**	56.7 %	4,220.9%	3.8 %
North America	363,224,006	4.8 %	**320,068,243**	88.1 %	196.1%	8.6 %
Oceania / Australia	40,479,846	0.5 %	**27,549,054**	68.1 %	261.5%	0.7 %
WORLD TOTAL	**7,519,028,970**	**100.0 %**	**3,739,698,500**	**49.7 %**	**936.0%**	**100.0 %**

NOTES: (1) Internet Usage and World Population Statistics updated as of March 31, 2017. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations - Population Division. (4) Internet usage information comes from data published by Nielsen Online, by ITU, the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) Information from this site may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2017, Miniwatts Marketing Group. All rights reserved worldwide.



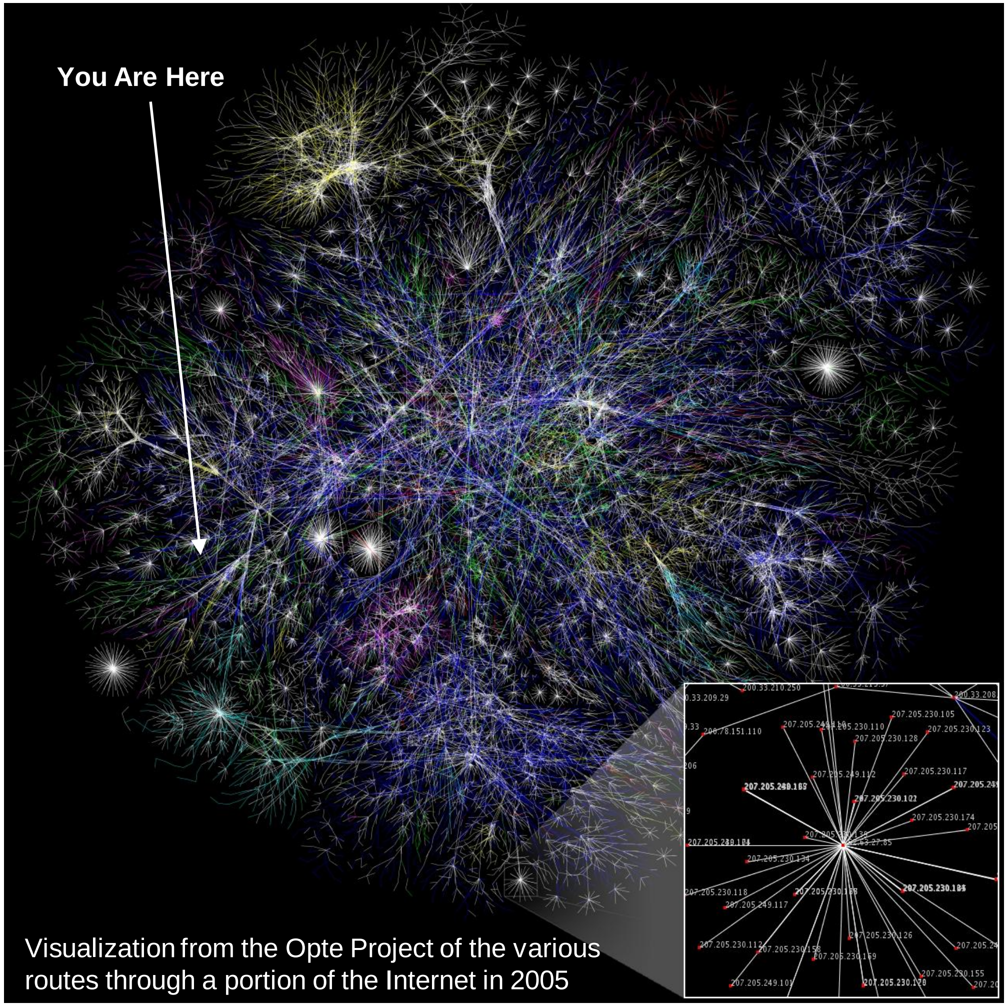
Internet World Penetration Rates
by Geographic Regions - 2017 Q1

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,519,028,970 and 3,739,698,500 estimated Internet users for March 31, 2017.
Copyright © 2017, Miniwatts Marketing Group



Internet Users in the World
by Geographic Regions - 2017 Q1

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,739,698,500 Internet users estimated for March 31, 2017
Copyright © 2017, Miniwatts Marketing Group



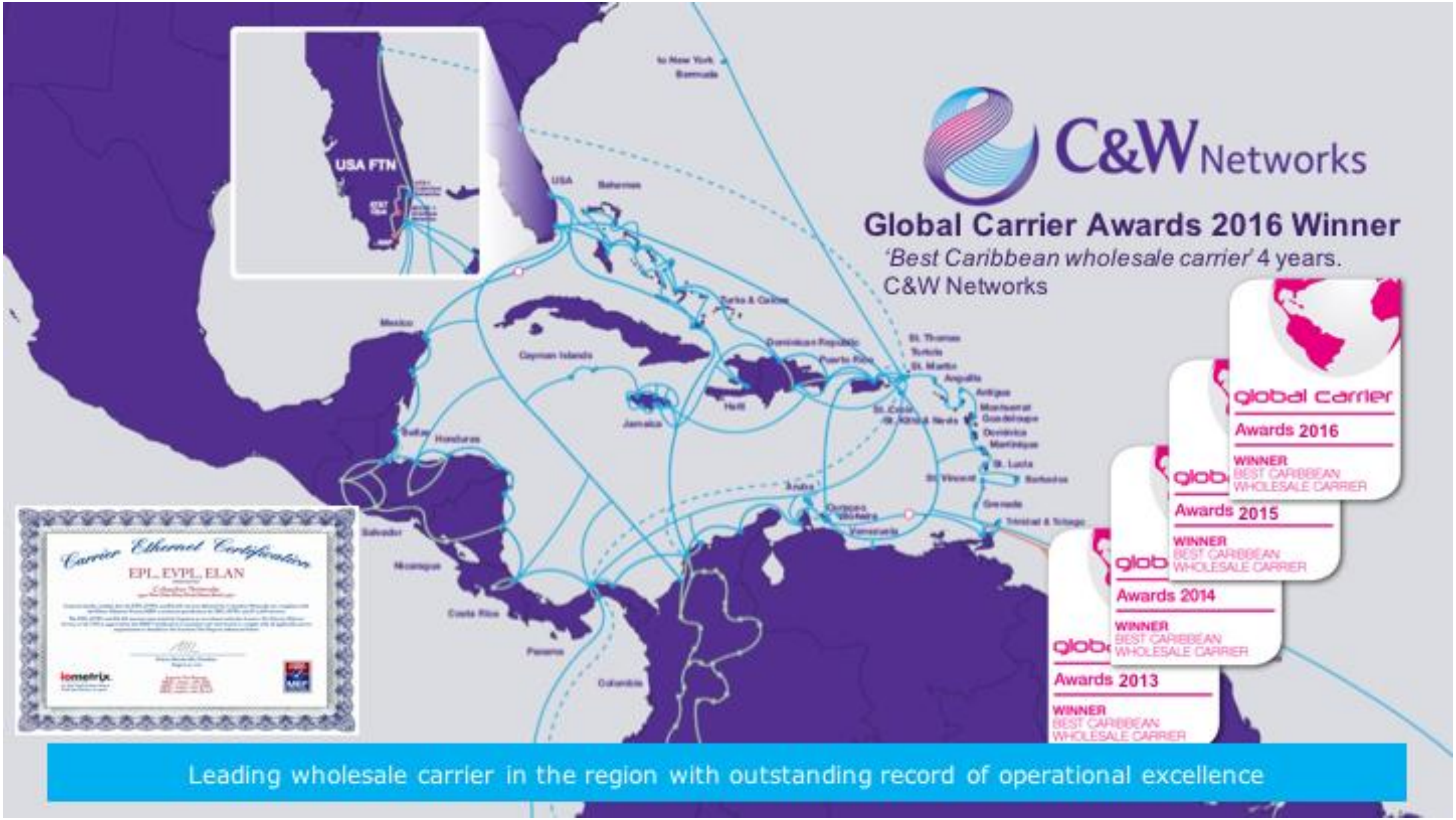
You Are Here

Visualization from the Opte Project of the various routes through a portion of the Internet in 2005

Source:http://www.internetworldstats.com/stats.htm

C&W SP Network

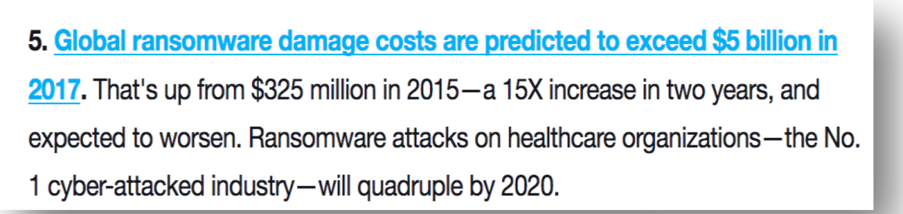
C&W Networks – Largest carrier of Internet Traffic for Caribbean and LatAm



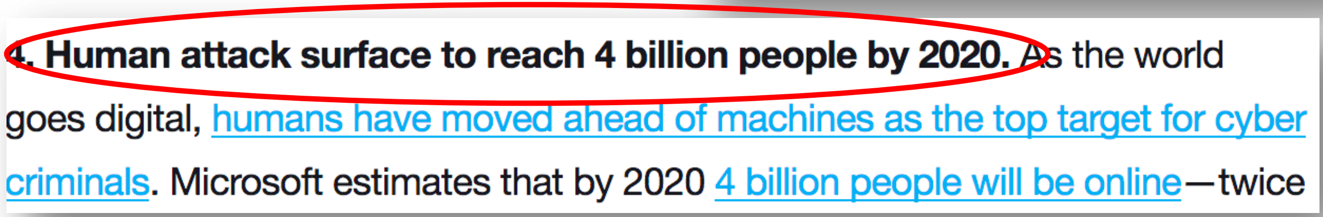
Cyber Security: A Growing Business

Indisputable: Cyber Crime is growing

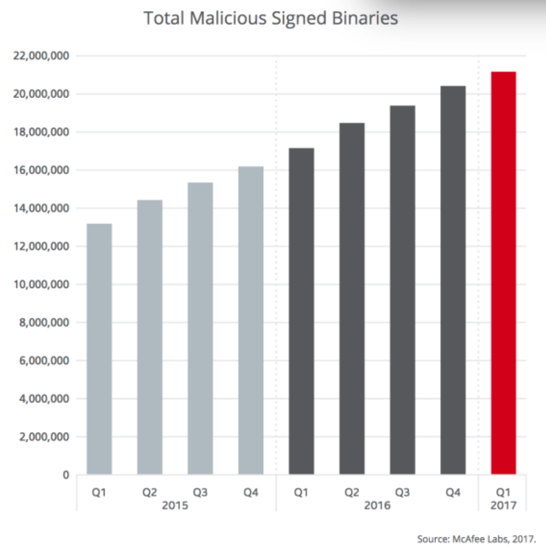
Outlook to 2021	
Market Size	Annual Spend Est: $1T Damage Est: $6T



5. **Global ransomware damage costs are predicted to exceed $5 billion in 2017**. That's up from $325 million in 2015—a 15X increase in two years, and expected to worsen. Ransomware attacks on healthcare organizations—the No. 1 cyber-attacked industry—will quadruple by 2020.

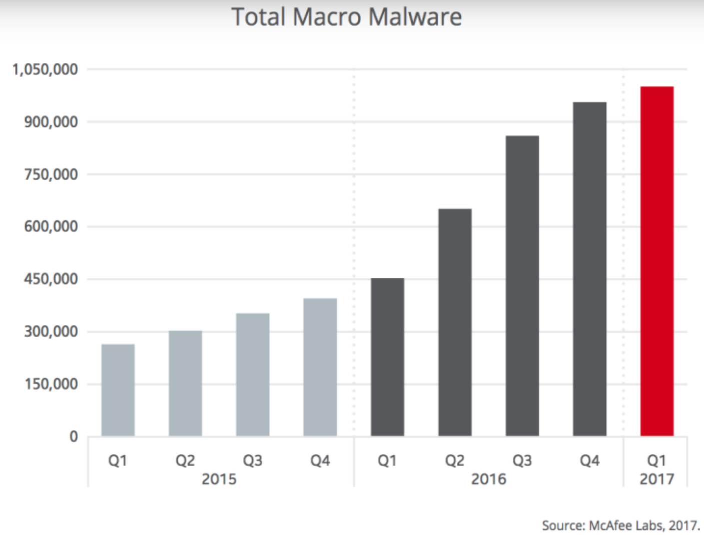


4. Human attack surface to reach 4 billion people by 2020. As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. Microsoft estimates that by 2020 4 billion people will be online—twice



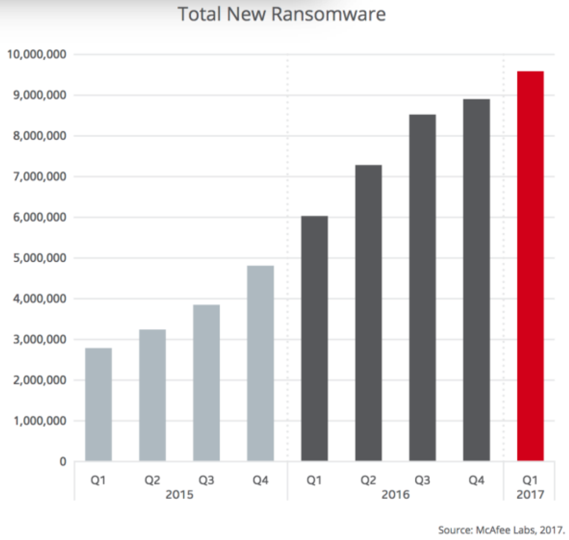
Total Malicious Signed Binaries

Source: McAfee Labs, 2017.



Total Macro Malware

Source: McAfee Labs, 2017.



Total New Ransomware

Source: McAfee Labs, 2017.

https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

Service Provider - Cyber Security Threats

Who is the biggest risk?

хакер

POTUS:
"No computer is safe! Use a courier instead"

Cyber Security: Who is the Target?

LIBERTY GLOBAL

Primary Target of Attack: ISPs, Subscribers, Devices and Applications

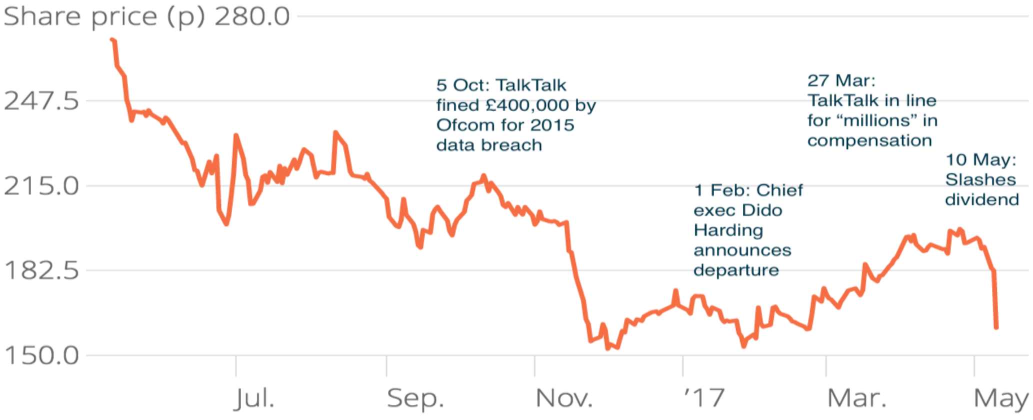
1
Service Providers

- Service Theft
- Service Attacks
- Spamming
- Data Theft
- Reputation
- Revenue Loss
- Regulatory Fines

2
Customers

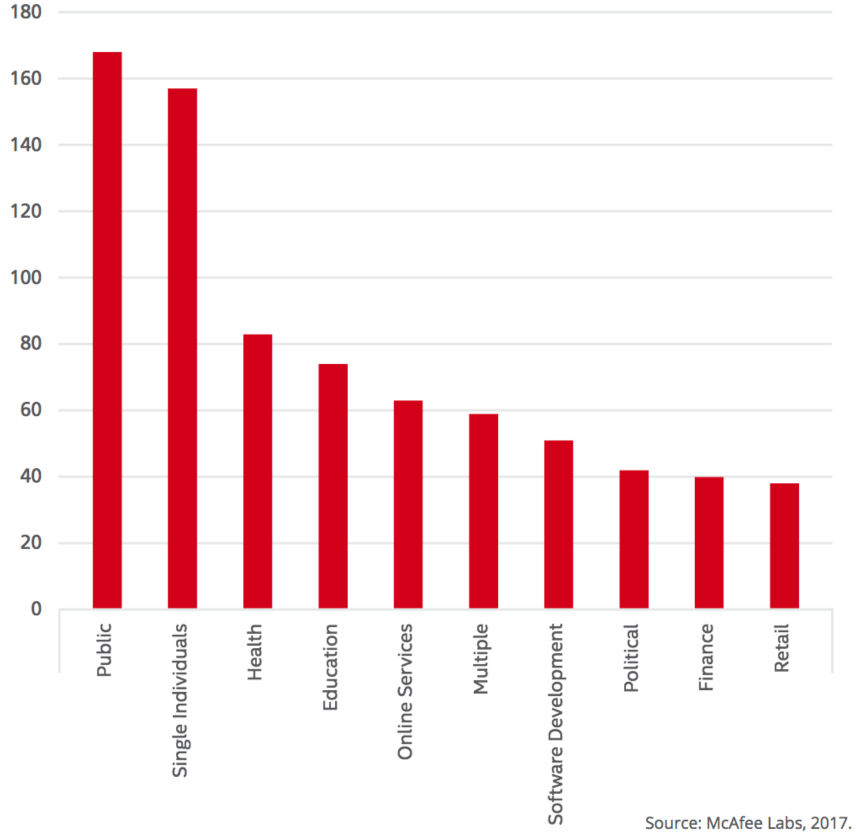
- Viruses
- Malware
- BOTs
- Privacy
- Identity Theft
- Phishing

TalkTalk: Time for "new priorities"?



Made with Chartbuilder

Top 10 Targeted Sectors in 2016–2017
(number of publicly disclosed security incidents)

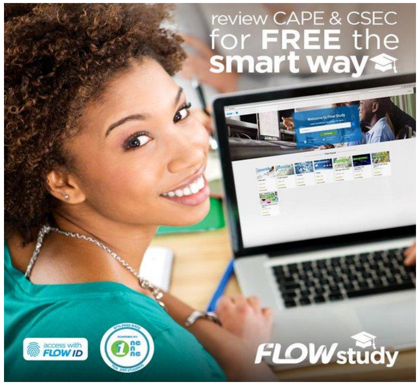


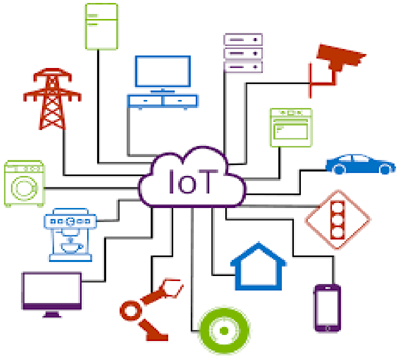
Source: McAfee Labs, 2017.

https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

SP: Customer Security Education

Customer First: SP’s Must Promote Safer Computing





A well-educated user will go a long way on the threat landscape. Educate and empower users to navigate the web safely.

Safe computing starts with:

- Anti-Virus Program - Have an Anti-Virus installed and keep application software and virus definitions updated.
- Software updates - All Software especially Microsoft updates should performed regularly.
- Secure Password - Change all passwords frequently. Force password changes at least once a year on account/bill payment site, email account and any other password.
- Privacy - Protect your Privacy by not providing your personal information over the internet.
- Backups - Have an offline backup of operating system and files.
- Online Scams - Scammers send phishing emails to trick the recipient of the email to click on a malicious link. Such link will be used to compromise the user’s account or capture the user’s information. At same time not to respond to emails requesting personal email from unknown sources and mark them as junk.
- Mobile Protection - Make sure your cell phone is regularly updated. Do not connect your phone to any unknown open wifi. If you do connect to an open wifi, do not access secure websites such as your banks online portal.
- Advise consumer not to send usernames, password or any other sensitive information via email. A phone call or an in-person conversation can save them from identity theft.

LIBERTY GLOBAL

SP Role in Mitigating / Inhibiting Attacks

Adopting a Strategy to Support the Customer

SP: Most Control / Least Effective

Service Provider Network
- Network Control
- Filtering
- DDoS Mitigation
- Monitoring
- Infra Protection

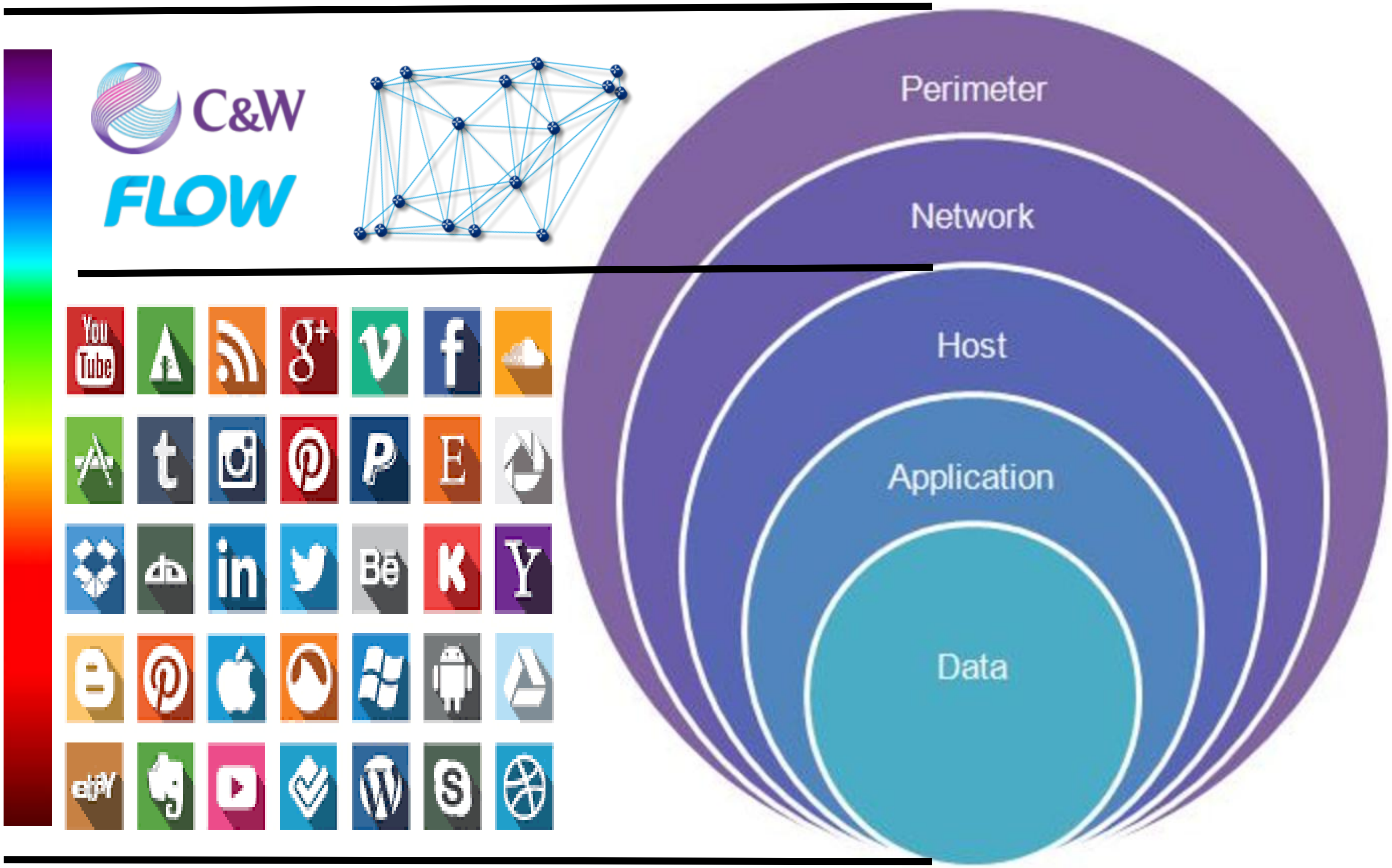
Customer Network
- Open WIFI
- No Filtering
- No Firewall
- No Monitoring
- Simple Passwords

Customer Equipment
- Computers
- Cell Phones
- Tablets
- Smart Home Devices
- Internet TVs
- Weak Password
- Customer Patching

Customer Applications
- Delegated Access
- Weak Password Policy

SP: Least Control / Most Effective

Defense in Depth Strategy



Cyber Security: Perimeter Protection

LIBERTY GLOBAL

Secure Network Perimeter Architecture

- Requires multiple layers of defense
- Up-to-date and hardened policies
- Proper controls and segmentation.

- Layers impede attacker advancement
- Allows more time to identify threats
- More time to react and minimize impact

Perimeter 1

Service Provider:

1. CGNAT
2. SIEMs
3. HoneyPots
4. Sink Holes
5. IP/Route Filtering

Perimeter 2

Enterprise/Subscriber:

1. Firewalls
2. Web Filtering
3. IPS/IDS

Perimeter 3

Host & O/S Protection

1. Advance Malware Protection
2. Identity awareness
3. Application Control

Case Study: WannaCry Ransomware

The Cost?

Size of Business:

Servers: 300+
Workstations: 1k to 4K

Man Hours to Patch (Avg):

Manually (45 min Avg): 2000+
Automated Tools (15 Mins): 645

Cost to Patch (Labour):

Manually (45 min Avg): $20,000
Automated Tools (15 Mins): $6,450
Total Ransom collected was $72k

$=?

Industry Outlook:
Ransomware $5B Impact in 2017

Lessons Learned?

- **Prevention saves Time & Money**
  - Most organizations do not patch proactively
  - Documentation and clients' status: Unknown
  - WannaCry exploit came weeks after Microsoft released a patch!
- **Re-active patching cost way more!**
  - Unless well prepared expect ***IT Staff*** to be engulfed / overwhelmed
  - 2000+ man-hours does not happen in a 24 hour period or over a weekend
- **Recovery is even more expensive!**
  - BitCoins = Real Money
  - Data-Recovery is expensive
  - Data-Loss is even more expensive
  - Paying ransomware exacerbates the problem - bad guy incentive
  - WannaCry decryption starting price $300
  - Ransom price increases the longer you take to pay

Source: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

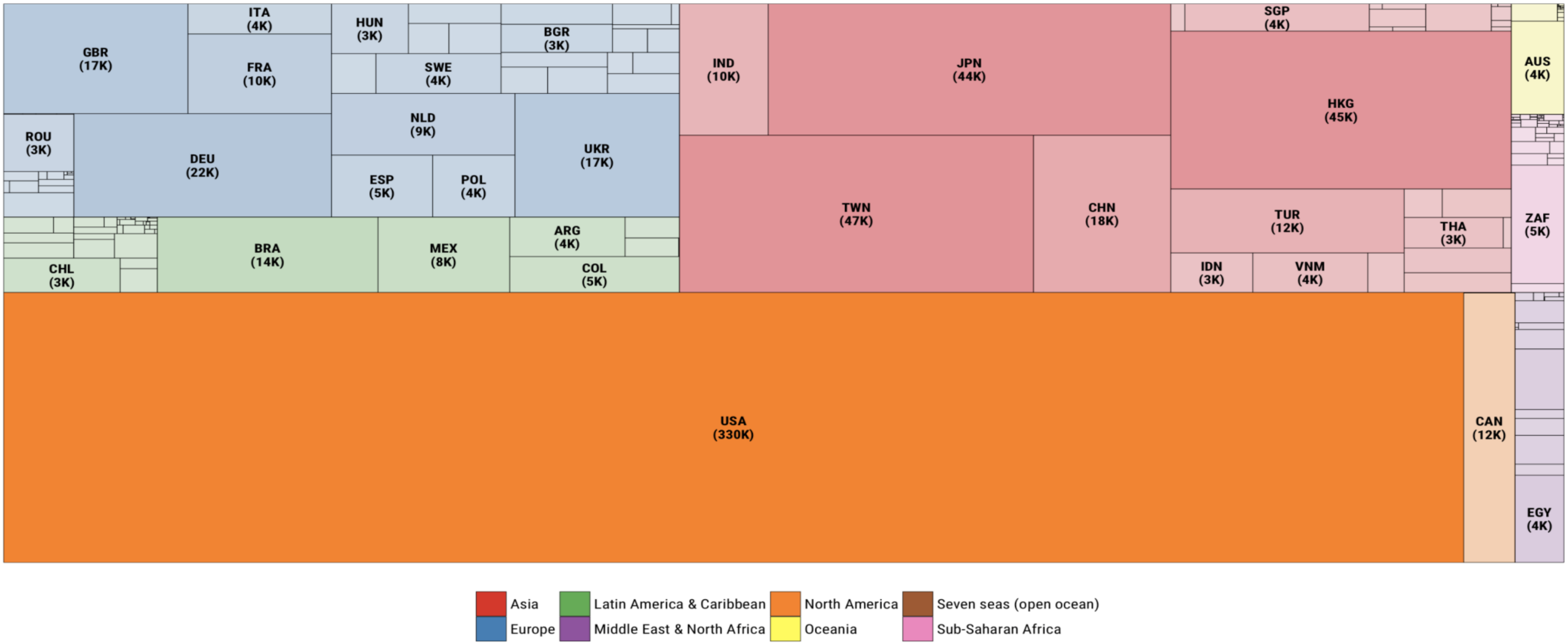
Case Study – WannaCry

Recent threat – Wannacry and SMB Exposure

The following is an example of the constant threat for any internet exposed infrastructure. CWC/LG Internal tools correlated the following data on the Country-level distribution of Windows nodes exposing SMB activity.

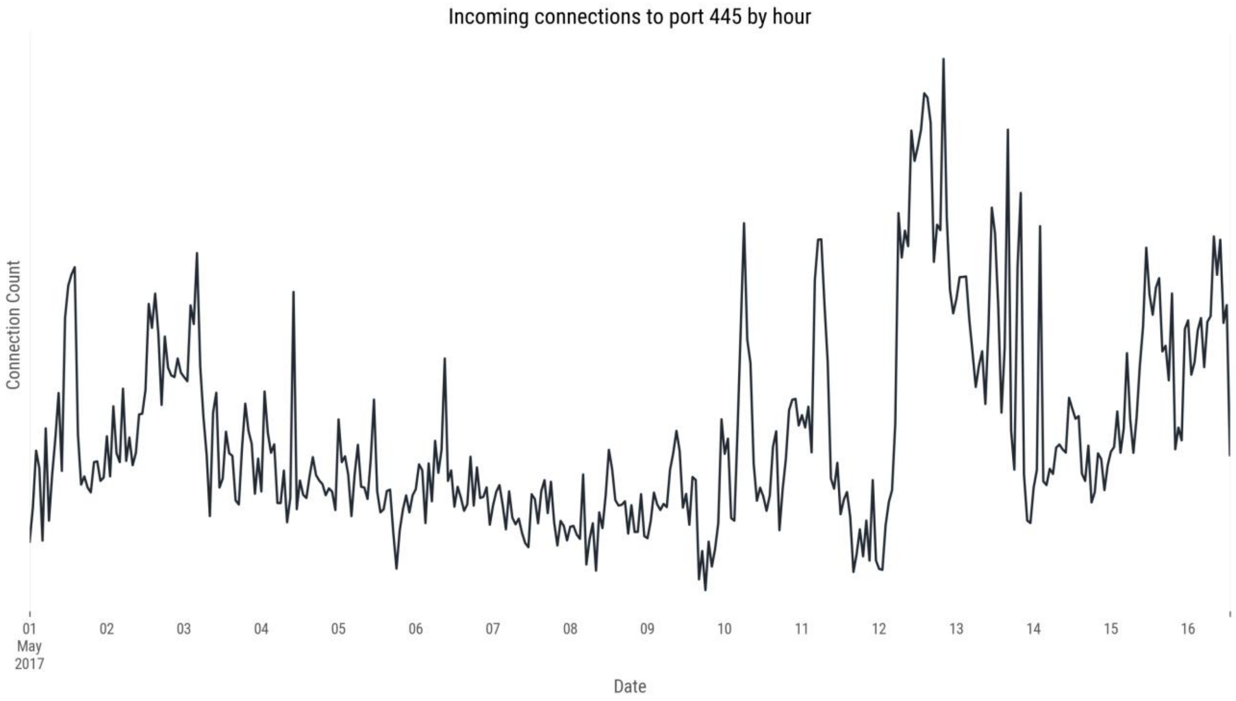
Country-level distribution of Windows nodes exposing SMB (port 445)

Hosts were classified using Rapid7's 'Recog' utility - https://github.com/rapid7/recog



Case Study – WannaCry

- Internet scanning and attempted connections are constant.
- Project Heisenberg is a collection of honeypots distributed around the world
- Designed to monitor the Internet to learn about scanning activity, the data shows the incoming connections to port 445 for the first half of May 2017.
- In the case of the recent Wannacry attack, spiking can be seen on May 10th and 11th, with a larger spike observed on May 12th as malicious actors attempted exploitation of the SMB MS17-010 vulnerability.



SP: Customer Security Education

LIBERTY GLOBAL

At a minimum, all customer should have host level defense including:

1. Anti-Virus (updated regularly)
2. Operating System patches – Automated and updated
3. Software/Application patches – Automated and updated
4. Host IPS/IDS – Automated signature updates
5. Host Firewalls Enabled
6. Only required IP Ports should be opened
7. All communications channels should be encrypted
8. Embrace IPV6!

Reality: *"Security is complicated, technology is getting more complicated, Cyber threats are sophisticated, customers will always be a SP's greatest risk"*

C&W Network Operations & Customer Service

C&W Approach

- Our networks have multiple levels to identify and manage:

Distributed SIEMs	Multiple NOCs
Proactive Monitoring	Distributed SOC
DDOS Mitigation Tools	Incident Management

- Our NOCs Monitor Malicious Activity, Block known malicious sites or attempted connections for known vulnerabilities.

- Customer Support is critical:
  - Bulletins - become more proactive and send customers notifications of known security updates or ransomware attacks.
  - Technical Support is a key part of our strategy for both Consumer and Enterprise customers

- Data Breaches - Part of data breaches is why we should care about our privacy. Hackers and criminals target companies and users to obtain data about an individual. We are typically the first point of contact for help on these threats, email, ransomware, etc.

- Our Front Line Staff and NOCs are an integral part of our Cyber Security Response Team, internally and externally.