THE CHANNEL

| Channel Issues and Advice |

August 2015

Contents

THE CHANNEL has been designed specifically for senior-level channel executives. It provides guidance and highly strategic advice on the channels and what senior channel executives should be aware of. It will guide management teams on the impact of competitor announcements, insights into the market, brief focus on services sub-segments, value stack, vertical focus and key director messages.

1 SLA – Senior Level Advisory

Founder & CEO
Robert Herjavec

Robert Herjavec is a dynamic entrepreneur who is featured on the US version of ABC network's Shark Tank (equivalent to the UK's Dragon's Den Format). He and our executive team are frequently asked to comment on the latest cyber threats and breaches within the US and Canadian markets. In fact, Robert was recently profiled in Forbes magazine - http://www.forbes.com/sites/davidparnell/2015/06/22/shark-tank-robert-herjavec-how-to-tell-if-you-are-cyber-secure/

Herjavec Group

Dynamic IT entrepreneur Robert Herjavec founded Herjavec Group in 2003, and it quickly became one of North America's fastest-growing technology companies, accelerating from $400K to $140 million in sales annually over 12 years. Herjavec Group delivers managed security services globally supported by a state-of-the-art, PCI compliant Security Operations Centre (SOC), operated 24/7/365 by certified security professionals. This expertise is coupled with a leadership position across a wide range of functions including compliance, risk management & incident response. Herjavec Group has offices globally including three headquarters in Toronto (Canada), New York City (USA) and Reading (United Kingdom).

Expansion into Europe

Herjavec Group acquired UK-based Sysec in Q1 2015. Sysec™, a leading IT security solutions provider and the 2014 McAfee EMEA Accredited Certified Engineer (ACE) Partner of the Year has been successfully integrated and rebranded as Herjavec Group. Today Herjavec Group UK continues to service over 200 enterprise clients across the UK and is elevating its offering of Managed Security Services. A London based Security Operations Center is slated for development by Q1 2016

Business Breakdown

	2015
Revenue	$140M

Consult – Security Consulting Services Team reviews infrastructure architecture, preventative controls and detective controls in order to assess the environment's security.
Deliver – offers installation services, design & migration support and project management.
Manage – 24x7x365 - on prem, cloud or hybrid managed solutions
Remediate – services are modelled after NIST SP800-61r2 and ISO 27035 with three tiers of support driving client communication, project scope, quality assurance and incident response

Recognition

Herjavec Group was recently recognized as #23 on the Cybersecurity 500 ranking (http://cybersecurityventures.com/cybersecurity-500/). This listing creates awareness and recognition for the most innovative cybersecurity companies who provide products and services. Of note, only 4 companies within the top 25 offer Managed Security Services and Herjavec Group are the only firm laser focused on security within that elite group.

Herjavec Group has also been recognized as:

- 2014 Canadian Palo Alto Networks Partner of the Year
- 2014 RSA Top Managed Services Win
- 2014 McAfee EMEA Certified Engineer (ACE) Partner of the Year

Herjavec Group's key area of differentiation is in its high touch managed services offering. It focuses on meaningful security use cases to proactively identify attacks. The Herjavec alert framework is applied in addition to client specific use cases to the onboarded technology across the following key attack categories: authentication, targeted attacks, malware, DDOS, and traffic anomalies. Once an alert is received by the Herjavec Group Analytics Platform, a series of automatic functions is performed to prepare a readable output for our analysts.

These functions include:
Cross-client Correlation: Herjavec compares alert types within a client environment across all clients. The output shows which attackers are targeting multiple clients, resulting in immediate escalations.
Trending: Herjavec develops trend lines that compare the immediate occurrence of any given alert with historical volumes of that alert over the past 4 hours, 24 hours, 7 days and 30 days
IP Reputation Scoring: Herjavec correlates the source address with known adversaries
Anomaly Detection: Herjavec Analytics Platform can identify behavioural based events using machine learning technology.
Aggregation: all alerts are collected into a single platform facilitating centralized data enrichment, automated intelligence and analysis.
De Duplication: Suppression of multiple messages of a recognized alert

Herjavec core managed security services include:

- Intrusion prevention and detection
- Application security
- Next generation firewall
- Endpoint protection
- Data loss prevention
- Web proxy and URL filtering
- Vulnerability management
- File integrity monitoring
- Executive reporting

Vendor relationships

Analysis

Herjavec Group has managed the transition to Managed Security Service provision by organic and by acquisition (Metacomm and Cyberklix) and another two acquisitions have given it geographic expansion (Galaxy Tech in the US and Sysec in the UK). It is well positioned to utilise the MSSP model to aid subsequent expansion.

NEXT >
2) Key Announcement Implication

2 Key Announcement Implications

French businesses have an opportunity to capture billions of euros in additional revenue by expanding the country's digital economy to its full potential. A recent McKinsey study, finds French companies that have undergone thorough digital transformations may unlock revenue gains of up to 40 per cent, while companies that do not quickly become digitally integrated could lose up to 20 per cent of revenue to competitors. The report finds that consumer demand is driving the digital opportunity in France, and companies need to catch up. Some 80 per cent of the French population is online and have made France one of Europe's online sales leaders. The country scores high in smartphone and tablet sales, and its "digital GDP"—the sum of digitally driven economic activity—has grown in the past three years from 3.2 per cent to 5.5 per cent of total GDP, or by more than €110B. Yet among digital peer countries reviewed in the study, France ranks only in the middle of the pack in its digital evolution. While France shows advantages in some areas, such as fixed broadband penetration, it under-performs in others, including Internet

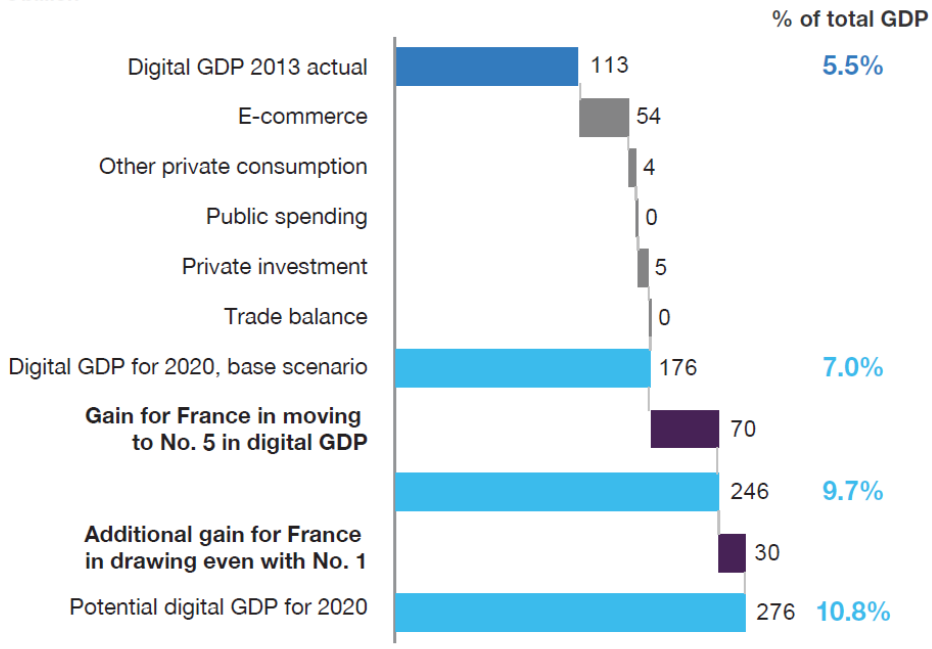
Closing France's €100B digital gap

Accelerating the country's rate of digital adoption could unlock billions of euros in economic value. The key is in executing a comprehensive digital transformation

Accelerating the digital shift

While digital transformations require businesses to commit intellectual and material resources, the bottom line is that growth opportunities will move on unless French companies are to meet the digital demands of consumers and business partners. Our survey of 500 French firms highlighted four main reasons for this relatively slow pace of digital adoption: organizational inflexibility, a lack of digital talent, tight margins that hamper investments, and the absence of top-management leadership. Addressing these could enable a speedier digital transformation that would unlock billions of euros. If France shifts into a higher gear equal to the rate of the top five in its peer group, the country could reap an additional €70B by 2020 (exhibit). If it equaled the United Kingdom, Europe's digital leader, the total digital gain could be €100B.

Exhibit By matching levels attained by Japan (No. 5) or South Korea (No.1), France (No. 8) could gain €70 billion or €100 billion in digital GDP.



Note: scope is the GB countries + Brazil, China, South Korea, India, and Sweden.
Source: McKinsey analysis

speed. Of greater concern is that a significant gap exists in business usage. Only 14 per cent of French companies took online orders in 2013, compared with 26 per cent of German companies, while only 65 per cent of French companies have a website, compared with 89 per cent in Sweden. Digital progress in France is essentially in a middle gear, with digital GDP likely to grow to 6 per cent of overall GDP in 2016 (worth €135B) and 7 per cent by 2020 (€180B) unless changes are made.

Investments in France announced in 2015

"…digital innovation will be undertaken thanks to a $100M investment from Cisco in French startups" said a statement from French Prime Minister Manuel Valls' office after he met with the company's CEO, John Chambers

Two weeks after announcing that it would scale up its activities in France with a new R&D center by 2016, Huawei's president presented to PM Valls a €1.5B investment over 3-years in the French market, focusing on its smartphone business

What would be needed to accomplish such a shift? The main ingredient is closer collaboration between stakeholders—the government, institutions of higher learning, private companies, and civil society

The French state can help raise the level of ambition among French businesses for a digital transformation through measures such as reducing the tax burden for digital investment, offering public contracts to stimulate digital innovation, securing development for very-highspeed fixed and mobile broadband, and introducing creative digital curricula in middle and high schools.

The *grandes écoles* and universities can deepen their investment in tomorrow's digital talent by furthering research in the cognitive sciences and semantics for data mining, as well as in artificial intelligence, robotics, and ergonomics, while discussing with private companies how best to anticipate future job needs.

Large corporations can set an example with their own digital transformations and by investing in digital partnerships with small- to medium-sized enterprises; their financial know-how could allow them to act as venture capitalists, backing the start-up-driven digital ecosystem.

Civil society, including employer and employee organizations, have dense, well-structured networks, which could be very effective in spreading digital knowledge, deploying digital coaches and mentors to companies throughout the country, and organizing conferences to raise awareness about the possibilities opened up by digital transformations.

Conclusion

These efforts could be usefully supported at the European level, within the framework of the European Union's growth policies. Investments made by EU member states in digital infrastructure and technology, for example, could be excluded from the public-spending calculation used in the Growth and Stability Pact. Ultimately, the risks generated by digitization (such as personal-data protection issues or loss of data sovereignty) must be addressed to avoid jeopardizing the potential gains.

Consumers are increasingly expecting a rich customer experience. At the same time, digitization is boosting consumer purchasing power with new free services while greatly improving the availability of quality products and services. Stakes are high. The disruption caused by digitization can create or destroy significant value for companies, depending on their starting positions and how well they respond to shifting consumer behaviour and other trends. Observed bottom-line impact has ranged between 20 percent revenue loss and 40 percent gain. Business experience across diverse industries demonstrates, however, that the opportunities outweigh the risks. French companies that deliberately and effectively implement comprehensive digital transformations will be able to capture most of the benefits linked to this historic economic pivot while avoiding the pitfalls.

To download the full French-language report, visit the McKinsey France website at mckinsey.com/global_locations/europe_and_middleeast/france/en

NEXT >
3) In Depth Focus

3 In Depth Focus

Dimension Data Network Barometer

The study comprised of 350 (288 in 2014) Technology Lifecycle Management Assessments globally discovering nearly 70,000 devices and support services data gathered from four Global Services Centres (Bangalore Frankfurt, Boston, and Johannesburg) from which 175,000 service incidents in 105 countries

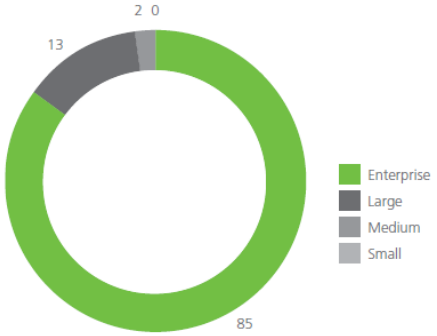
The Dimension Data Network Barometer reviews the status of networks globally

Aggregates data from the 350 Technology Lifecycle Management (TLM) Assessments conducted across the world in 2014 and compares them to the data from the past 6 years

While the obsolete devices may therefore be more secure, the risk is that vendors won't provide assistance with any new vulnerabilities discovered on these devices, as the technology has passed its last day of support

Sample

The sample is well represented geographically although MEA was primarily South Africa



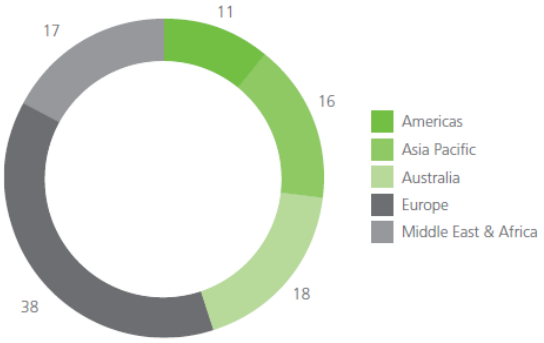


Fig 1 Sample distribution – Enterprise >2500 users Fig 2 Geography (Percentage)

Vertical Industry

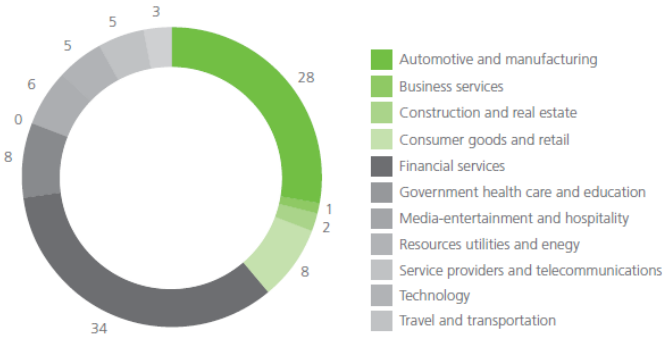


Fig 3 Vertical Industries (percentage)

The report gives a good representation across 11 industries

Two verticals made up over half the sample – Financial Services and Automotive and Manufacturing. Government was significantly down

Average mean time to repair on current equipment is 4.2 hours compared to 3.3 hours for obsolete equipment

Assessment

Considering the vulnerability of devices by lifecycle stage obsolete devices have 2 per cent fewer security advisories than current devices while ageing

There's been a slight improvement in the security status of networks this year: the percentage of devices with at least one vulnerability is down to 60 per cent from 74 per cent last year
Almost 1/3 of incidents are caused by human error, therefore avoidable through proper configuration and change management tools and processes

Key security capabilities to consider:
• visibility and discovery tools – both network- and application-based
• incident response plans and automated workflow
• vulnerability and remediation management
• risk profiling appropriate to business context
• network-, application-, and data-centric protection controls that can be rapidly applied when risks are discovered and assessed

devices have a 5 per cent more security advisories than current devices. Current devices haven't been in the market long enough to be tested comprehensively by security researchers. But as time passes, devices are exposed to more testing, and even attacks, which would increase their number of known vulnerabilities.

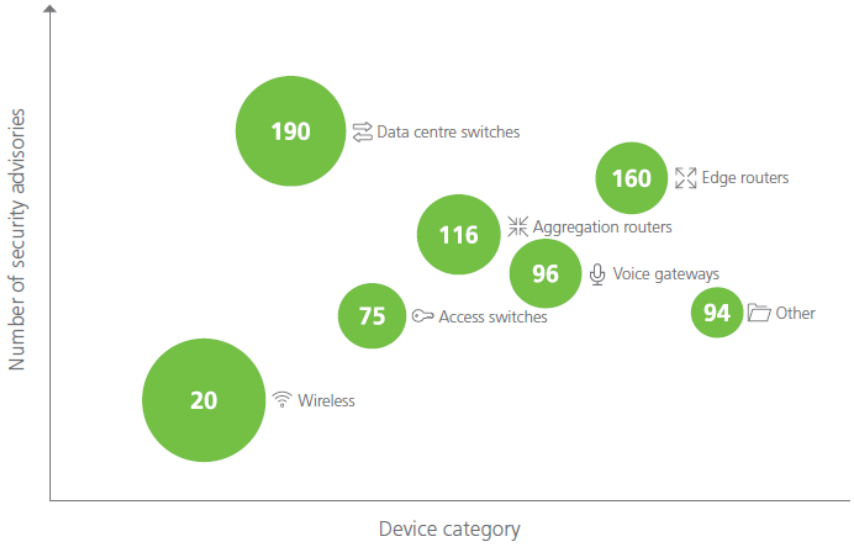


Fig 4 Number and penetration rate of security advisories by device type

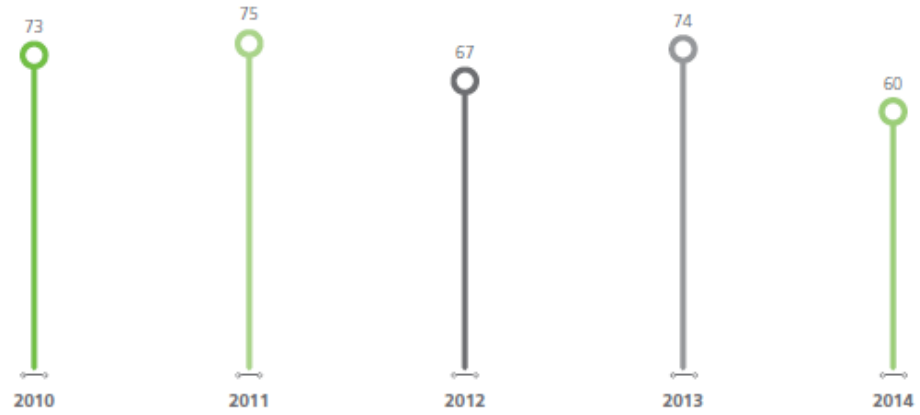


Fig 5 Percentage of devices with at least one vulnerability, global average

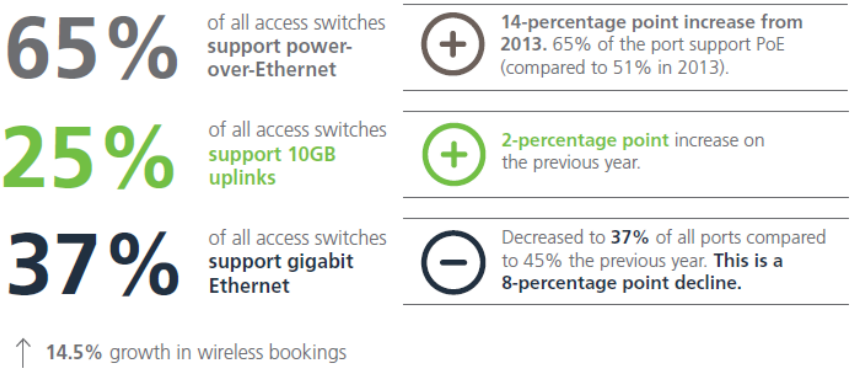


Fig 6 Network access point wireless capabilities

Only devices with the later model numbers 802.11n and 802.11ac can fully support wireless connectivity. However, there were no 802.11ac devices discovered this year, and only 26 per cent of discovered devices were of the 802.11n type. This implies that the vast majority of network devices (74 per cent) are still not able to support advanced wireless and mobility requirements. This data also explains why there's still so much access switching infrastructure that doesn't support power-over-Ethernet, gigabit Ethernet, and 10-gigabit uplinks: most access points are still of the 802.11g variety, which only delivers a theoretical maximum throughput of 54Mbps. While not strictly an architectural trend like enterprise mobility, the Internet of Things is also predicted to have an influence on corporate infrastructures, particularly in the adoption of the new Internet protocol, IPv6, across network devices

For a copy of the full Didata slide deck and report please send a request to info@eurolanresearch.com

Results show that only 21 per cent of devices currently support IPv6. The largest proportion of devices (48 per cent) can be switched to IPv6 through a simple software upgrade, but currently remain as is, which again indicates a lack of basic network maintenance.

Mobility

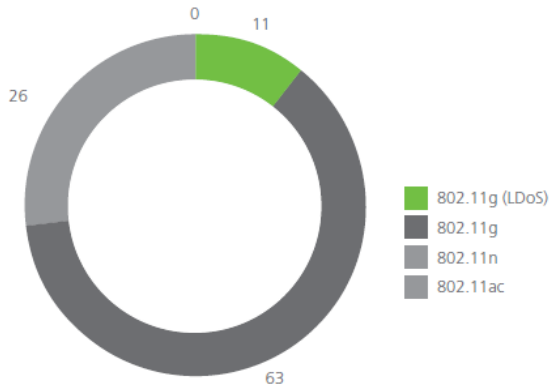


Fig 7 Percentage of devices that support mobility

Recommendations

Improve operational support maturity level by considering the following four steps:

1. Achieve maximum visibility of your entire networking estate.
Create and maintain an accurate inventory of all networking devices in your estate, their lifecycle stage and position within the network, known security vulnerabilities, and criticality to the network's overall uptime.

2. Standardise the types of technologies used in your network, as well as their configurations, as much as possible. A greater degree of standardisation will reduce not only risk in terms of fewer possible operating system vulnerabilities and configuration errors, but also reduced support costs and average time to repair, should devices fail

3. Automate as many of your day-to-day management tasks as possible.
Automation is dependent on standardisation. Automating simple tasks such as configuration management, password change management, configuration backups, or other scheduled maintenance tasks will help to reduce human error, thereby increasing the efficiency with which your network is maintained and supported. Investigate various options such as managed services delivered by a competent services partner, or even moving to a software-defined network

4. Monitor your network devices more closely and proactively.
This could be achieved through either internal or outsourced remote monitoring services. Proactive monitoring of devices can help predict when devices may fail, and reduces the time it takes to troubleshoot and repair faulty devices. Consider allowing your support provider to monitor the devices it supports

NEXT >
4) Financial Roundup

4 Financial Roundup

	Income $M	Latest quarter Sales $M	
Arista	24.0	195.6	↗
Cisco	2319.0	12843.0	↗
Brocade	91.7	551.9	→
Juniper	158.0	1222.2	→
Mitel	-37.3	282.3	↘
Extreme	-15.7	149.9	↘
Avaya	-49.0	999.0	↘
DLink	-4.1	198.6	↘
Netgear	3.7	288.8	↘

Source: Company Financials - all based on latest released quarters ended June except Brocade and Cisco are July

Recently Released Financials

Arista Q215 – Growth of 42 per cent YoY and 9 per cent sequentially. The geographic breakdown:

- US 77 (75) per cent
- International 23 (25) per cent

Avaya Q315 – Growth was down 11 per cent YoY and down 6 per cent sequentially. The geographic breakdown:

- US 54 (52) per cent
- EMEA 26 (28) per cent
- Asia 11 (10) per cent
- ROW 9 (10) per cent

Brocade Q315 – Growth of 1 per cent YoY and sequentially. The geographic breakdown:

- International 43 (44) per cent
- North America 57 (56) per cent

Cisco Q415 – 1st quarter with Chuck Robbins as CEO; sales up 4 per cent YoY and 6 per cent MoM. Geographic breakdown was:

- US and Canada 61 (59) per cent
- Europe 24 (25) per cent
- APAC incl Japan 15 (16) per cent

D-Link Q215 – Growth was down 11 per cent YoY and 5 per cent sequentially. The geographic breakdown:

- EMEA 19 (21) per cent
- North America 20 (18) per cent
- AsiaPac 61 (61) per cent

Extreme Q415 – Down 3 per cent YoY. Geo breakdown:

- EMEA 37 (34) per cent
- Americas 50 (50) per cent
- AsiaPac and LATAM 13 (17) per cent

Juniper Q215 – Down 1 per cent YoY but up 15 per cent sequentially. The geographic breakdown:

- EMEA 26 (26) per cent
- Americas 60 (59) per cent
- AsiaPac 14 (15) per cent

Mitel Q215 – Down 2 per cent YoY. The geographic breakdown:

- EMEA 46 (42) per cent
- Americas 51 (54) per cent
- AsiaPac 9 (4) per cent

Netgear Q215 – Down 15 per cent YoY. The geo breakdown:

- EMEA 23 (30) per cent
- Americas 60 (56) per cent
- AsiaPac 17 (15) per cent

For further information, please contact:
Keith Humphreys – Managing Consultant at **euroLAN** – keith@eurolanresearch.com