Technology Brief...

March, 2016

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

INSIDE THIS ISSUE

Should Microsoft be in the PC Hardware Business?

Microsoft has made waves recently by releasing a higher-end notebook PC (Surface Book), setting it on a course to compete with its many key OEMs (e.g., Dell, HP, Lenovo, Acer, Asus, Samsung, LG) in a currently slumping market for PCs in general. While many see this as a troubling competitive strategy suggesting Microsoft is engaging in channel conflict with its OEMs, we see it differently. By its actions, Microsoft is actually helping to reinvigorate a moribund PC market.

Can Microsoft create a better PC?
The issue is not whether they can make a perfect PC. Surface Pro and Surface Book are not perfect implementations of notebook or 2 in 1 devices. The more important issue is, can Microsoft's move to design leadership and thought leadership of what a PC can be and therefore influence a market that seems dormant. The level of innovation has mostly been stagnant for several years, which is why sales have been slipping. Even Intel's influence on new product with its emphasis on Ultrabooks and hybrid computing solutions has not achieved anywhere near the success it should have. The innovation was not compelling and consumers responded accordingly. And yes, there was competition from smartphones and tablets, but this doesn't fully explain the slump in PC sales.

"…We recommend that Microsoft continue to make PC hardware, but only to the extent that it can produce truly innovative products that push the leading edge …pushing the market to be more competitive so that customers start buying PC devices again will ultimately benefit Microsoft and its total ecosystem...."

Microsoft's foray into the market with compelling products, were at first seen as competitive to their existing OEM base. But I would argue that rather than negatively affect them, it spurred them to attempt to outcompete Microsoft within the target markets Microsoft was addressing (the higher end of the PC market, especially the business market), and will ultimately help in the consumer space as well.

This is much the same strategy Google has used successfully with the Nexus line of smartphones and tablets. Google is not looking to put OEMs out of business. Rather, it is showing what can be done by pushing at some of the design limits and current levels of innovation. Further, by delivering its own products, Google gets direct feedback from customers about the features they like and dislike, as well as how the devices are used. This strategy will offer Microsoft the same benefits, and indeed it has already shown results. Last CES was full of examples of OEMs trying to out-compete Microsoft in the target markets of Surface Pro and Surface Books, and with some compelling new products that garnered a great deal of excitement. Examples of this are the recent launches of new HP EliteBooks and Dell Latitude/XPS devices.

Microsoft has been trying a similar strategy in the smartphone space, having purchased the Nokia phone business and trying to get the Windows phones markets invigorated, but now concentrating only on some key Lumia smartphones. But unlike in the PC space where Microsoft controls the vast majority of the market and its PC efforts have a huge base to attack, the market for Windows phone is miniscule (under 2%). As we've indicated previously, we don't believe Microsoft will be able to successfully increase this share given the overwhelming dominance of Android and iOS. But it can generate significant revenues in cross-platform app and services even if its Windows phone hardware business is a lost cause.

Bottom Line: We recommend that Microsoft continue to make PC hardware, but only to the extent that it can produce truly innovative products that push the leading edge of the market. Selling several million of its own units is fine, but pushing the market to be more competitive and to innovate so that customers start buying PC devices again will ultimately benefit Microsoft and its total ecosystem greatly.

Moving to Cognitive Security

The increasingly complex landscape of threats is leading to one conclusion – traditional methods of security such as user ID, password, anti-virus, and device lockdown, are not cutting it. With increasing sophistication of threat actors, the number and severity of attacks is increasing and the number being prevented is decreasing. To protect against a changing threat landscape, we need to look at security in a new way if we are to protect corporate data from loss.

Maximizing enterprise data security requires a continuum of actions. Detection is the one most organizations concentrate on with anti-virus and other on-client apps, but it's really just a first step and not an end by itself. Investigating the internal workings of the threat is the next level leading to an understanding of the threat necessary to cope with the danger. This offers an improvement in overall security, but it's not enough to stop here. It's important that we continuously learn about the intricacies of the threat and any changes it may undergo in the real world, as well as the goals of its implementer. We also need to be much better at knowledge sharing as it relates to threats to enable a wider base of information driving our actions, so each organization doesn't need to find each threat on its own. This is probably the single biggest challenge as very few companies, even at the vendor level, do this currently. Finally a response needs to be formulated based on the full analysis of the threat, and the subsequent assessment of how best to defeat it. Without all of these steps, the ability to deal with current threats and with more complex future threats will be limited.

"…Enterprises would do well to start looking at emerging cognitive based solutions for security, particularly as it relates to mobile and IoT devices. Old style anti-malware loaded on each device will not be sufficient to stem the threats now present and emerging. …

Figure 1: 5 steps to enhanced security

One of the primary needs going forward for threat detection and mitigation will be creating an intelligence based approach built on top of the security model outlined above by creating an analytics based approach. It's unlikely a manual process can

keep pace with all the changing and emerging threats. Fully automated cognitive computing solutions now emerging will learn in real time and can be highly protective.

Few enterprises currently realize how increased cognitive and analytics functions on mobile and fixed computers can result in far more secure environments. Knowing normative user behaviors allows limiting unexpected ones. Threat mitigation is related to cognitive learning about users and typical organizational uses. It includes expected pattern analysis between client and cloud, as well as learning about previous threat activities. It is similar to how the financial industry looks for anomalies in transaction history vs. behavior, raises flags when things look out of place, and takes action to contact customers and limit losses. The more we know about normative behavior the more likely organizations will find all the security anomalies it must to act on.

There are few security vendors that have the required technology and resources necessary to accomplish this task adequately. IBM, with its Watson initiative, and its extensive research and data base of threats, has an excellent opportunity to lead in this space, although it is still early in the maturity curve. Other companies, such as RSA, Symantec, and Intel, with their extensive knowledge of threats and their increasing use of cognitive/AI type tools, will also provide next generation security to their customers. This will be both for traditional fixed devices, but more importantly for current mobile and future IoT devices, where on-board tools may not be practical or insufficient to contain all threats. And it will entail an always connected device-cloud interaction to accomplish adequately. This will increasingly bring major networking vendors and carriers (e.g., AT&T, Verizon) to offer such services as well. And it's why Cisco has lately been making a number of moves into this space. We expect more vendors to do so.

Bottom Line: Enterprises would do well to start looking at emerging cognitive based solutions for security, particularly as it relates to mobile and IoT devices. Old style anti-malware loaded on each device will not be sufficient to stem the threats now present and emerging. Vendors are making progress in this space, but few enterprises have yet taken advantage of their capabilities. It is imperative they do so over the next 1-2 years by making the transition to new security threat avoidance and mitigation services, or face the potential for huge corporate losses.

Your PC has an Identity Crisis

"…the PC is the single largest point of risk for data leakage in business costing potentially millions of dollars per incident. The number of threats is growing, as is the vulnerability of organizations relying on old ways of providing security to their end user devices....."

Despite what some believe, the PC is not dead. Indeed it is still the number one business computing platform powering end user apps in most organizations. But is it safe? Despite our dependence, the PC is the single largest point of risk for data leakage in business costing potentially millions of dollars per incident. The number of threats is growing, as is the vulnerability of organizations relying on old ways of providing security to their end user devices. And organizations aren't sure what to do about it or what inaction costs.

To better understand the risks and what can be done to mitigate them, we recently released a research report, "Your PC has an Identity Crisis: Saving the cost of a hack and other benefits of enhanced identity". It analyzes the average cost of a PC hack, the percentage of hacks caused by credential loss, and the potential payback to enterprises that deploy hardware enhanced multi-factor authentication capability which is increasingly being build into the machines themselves.

Some of the key take aways from the research include:

- User name and Password are the primary login method currently used in 76.8% of companies, but will fall to 9.6% in the next 3 years
- In the next 3 years, Biometrics (47.2%), Phone based (38.4%) and Soft Tokens (32%) will dominate as required login credentials
- Our research shows that approximately 1/3 of companies know they have had a data breach, and it's likely that at least an equal number have had one without knowing it
- The average per employee cost of a data breach per incident is between $475 and $15,400, with an average of $7938.
- Based on the above, eliminating one incident by deploying a new, enhanced machine provides an ROI of 694%
- Credential theft represents approximately 45% of all threat actions against organizations, causing enterprises to take protective actions by regularly requiring password changes
- The cost per user in a typical organization forced to continuously change passwords as a result of threats is between $5055 and $6360 over a 3 year period.
- Eliminating the above provides an ROI of 505% to 636% per user

These are some of the conclusions of the research. A complete explanation of our conclusions and how we determined the various data points is included within the report. A complimentary copy of the full report showing the complete analysis is available upon request, by sending your request to sales@jgoldassociates.com.

Recent Research

Contact us to request the following research reports:

Market Studies

- **The State of Enterprise Mobile Management (EMM) 2015**
- **Mobile E-Commerce: Friend or Foe?**

2015 Emerging Technology Trends

- Highlights our key emerging trends for the next 2-3 years

Commentary and Analysis

- Apple and IBM in Enterprise: Joined at the Apps

Technology Reports

- Your PC has an Identity Crisis: Saving the cost of hacks and other benefits of enhanced identity
- Replacing Enterprise PCs: The Fallacy of the 3-4 Year Upgrade Cycle
- Keeping Notebooks Past Their Prime: A Study of Failures and Costs

Whitepapers

- A Heuristic Approach to Mobile Security
- MDM- Where Do We Go From Here?

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight

About J.Gold Associates, LLC.

J.Gold Associates provides advisory services, syndicated research, strategic consulting and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies. We work with our clients to produce successful new product strategies and deployments through workshops and reviews, business and strategic plan coaching and reviews, assistance in product selection and vendor evaluations, needs analysis, competitive analysis, and ongoing expertise transfer.

J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends in the computer and technology industries. We have acquired a broad based knowledge of the technology landscape and business deployment requirements, and bring that expertise to bear in our work. We cover the needs of business users in enterprise and SMB markets, plus focus on emerging consumer technologies that will quickly be re-purposed to business use.

We can provide your company with a trusted and expert resource to maximize your investments and minimize your risk. Please contact us to see how we can help you.