Multifaceted security: preparing your cyber offense
Theme #3: **Multifaceted security**

*Multifaceted security: preparing your cyber offense* is part of an EY *Top of Mind* series addressing four key themes that can help guide technology executives’ actions during this time of unprecedented disruption. Here we explore the need for companies to address the many vulnerabilities and threats multiplying amid technology transitions, by taking a multifaceted approach to cybersecurity, including cyber offense.

The four-theme series includes:

1. **Stack to solution** – technology stacks being displaced by cloud-integrated solutions
2. **Hunting for hidden gems** – pockets of innovation and troves of data lying untapped within the company
3. **Multifaceted security** – vulnerabilities and threats multiplying amid technology transitions
4. **In the crosshairs** – challenges proliferating from upstarts and activist shareholders

To access our collective overview of the four themes, go to: ey.com/technology.
All around the world, a rising tide of cybercrime is challenging companies in every industry – none more so than technology. It’s no longer a matter of “if” but “when” your company’s security is breached. So, to achieve true cyber confidence tech companies must act proactively and be prepared with flexible and resilient defenses, capable of responding to any cyber incident with speed and agility.

The same disruptive cloud and mobile technologies that enabled the digital transformations now sweeping through all industries have increased corporate networks’ cyber vulnerability. New kinds of cybercriminals have emerged to exploit that increased vulnerability. Nation-states with geopolitical motives, “hacktivists” with ideological motives, organized crime with financial motives and a modern cyber version of corporate espionage have replaced the stereotypical “prankster” hacker of old.

“In this new environment, all companies must look way beyond their IT infrastructure to fully understand their cyber risk. They must think more broadly about all their business relationships, and assess their cyber threat environment from economic and geopolitical perspectives as well,” explains Doree Keating, Transaction Diligence, Transaction Advisory Services, Ernst & Young LLP.

This is of particular importance to technology companies. Since technology increasingly underpins other global industries, tech companies make very attractive cybercrime targets. Therefore, tech companies need to be particularly diligent when addressing their own cyber risk profiles, as well as when building cyber defenses into their product and service solutions.

**Borderless networks give rise to multifaceted security challenges**

Vulnerability to information security challenges always increases during technology transitions. But the very nature of current disruptions raises security concerns to paramount importance. Borderless networks have replaced traditional closed and “private” enterprise networks, routinely storing confidential information, including intellectual property (IP), outside the perimeter of the corporate network, while also transmitting to mobile devices via open airwaves. At the same time, the nature of security threats is evolving, in part because the changes previously described lead to additional opportunities for exploitation.

“The new era gives bad actors more powerful opportunities and more potent tools with which to exploit those opportunities. So enterprises must become far more proactive about cybersecurity defense than many have been in the past – and they must develop an offense, too.”

**Jeff Liu**
Global Technology Industry Leader
Transaction Advisory Services
EY
Cyber offense: proactively “hunting” for intruders

While many organizations still need to overcome culturally ingrained lax security practices (such as poor password choice and indiscriminate document sharing), “most importantly, corporations must become proactive cyber hunters,” says Liu. “They should actively look for intruders in their environment, gather external threat intelligence and analyze what kind of threats are the likeliest to attack their organization. Will it be hackers seeking monetary gain, competitors seeking technology patents or trade secrets, or so-called hacktivists, who may disagree with something the company stands for?”

Recent research emphasizes Liu’s and Keating’s proactive cyber “hunting” message. A Ponemon Institute study found that a third (33%) of breached companies surveyed discovered their breach more than a year after the intruder had access to their environment, and another 20% could not determine how long their cyber enemies had access.¹ And in EY’s Global Information Security Survey 2015, 36% of respondents say that it is unlikely they would be able to detect a sophisticated cyber attack.²

Why tech companies attract cybercrime

The nature of technology companies makes them particularly attractive targets for cybercriminals. Financially motivated cyber intruders and those pursuing corporate espionage often seek to steal IP that includes technology patents but goes further, to manufacturing know-how, board books, business strategies, M&A target pipelines, negotiation strategies, etc. Technology companies, like all organizations, suffer risks to revenue, profit, market value, market share and brand reputation when hackers exploit such stolen IP.

¹ “2014: A Year Of Mega Breaches,” Ponemon Institute, January 2015, © 2015 Ponemon Institute LLC.

² Global Information Security Survey 2015, EY, © 2015 EYGM Ltd.
But technology company concerns can go further. If an intruder manages to insert malicious code in a tech product that is then sold to customers, that intruder could potentially infiltrate the far larger number of organizations represented by the tech company’s customer base. “If a tech company isn’t taking appropriate actions to protect and defend itself, it could be exposed to potential liability in that situation,” says Keating.

“It’s important for tech companies to understand this broader threat. These are typically sophisticated, long-term campaigns in which the hackers may not convert stolen information for months or even years. And the fix may not necessarily be just on the technical side,” she adds.

**What’s a tech company to do?**
Consequently, Liu and Keating recommend that technology companies proactively hunt for what cyber experts call “advanced persistent threats” (APTs) that may already be lurking in their corporate networks — or in the networks of their business partners and M&A targets.

An important part of the approach they recommend for uncovering APTs involves customized threat intelligence. Such analyses provide insights into who might be motivated to steal a given company’s IP (e.g., nation-states, organized crime, ideologues), what is known about each potential threat actor’s techniques and, therefore, what particular kinds of clues (known as indicators of compromise, or IOCs) to look for.

Keating explains: “Companies need to ask questions about their competitive economic situation and who might have interests in their market in order to assess who their attackers might be, what those attackers might be seeking and could they take something and then wait several years before actually using it.”

**Tech M&A demands special cyber threat analysis**
All tech companies should consider themselves under cyber attack all the time. But they must take extra special care in assessing potential cyber vulnerabilities associated with their acquisition targets — especially in light of the recent tech M&A boom back to dotcom-era levels. “Finding evidence of a cyber threat may undermine a deal — but acquiring a target with intruders that then infiltrate your network could undermine your business,” notes Liu.

Of note, tech company executive awareness of M&A-related cyber concerns is rising. EY’s December 2015 Capital Confidence Barometer (CCB) survey found that a majority (54%) of the 161 responding technology executives regard cybersecurity as a core part of their due diligence process (which involves not only the deal process but also a review of the target). Corporate vigilance definitely is increasing end to end as the vast majority (over 90%) of tech executives view cybersecurity as a significant risk (medium or high risk) to their deal process. And heightened media attention and this increased corporate awareness of the cyber risk are contributing to watchfulness at the C-suite and Board level.

Keating recommends tech companies view M&A-related cyber vulnerabilities from three perspectives:

- Thoroughly review each target’s business relationships, alliances and partnerships for potential threat actors who may be motivated to act against the buyer
- Forensically investigate the target’s IT environment for IOCs
- Take great care to protect the M&A process itself

---

**Cyber offense for M&A**

Keating emphasizes the first and third bullets. “M&A is one of the few times where all functional areas of an organization collaborate to understand and assess risk. With that, there’s a large amount of documentation going back and forth between the companies. That activity creates an extremely attractive opportunity for cyber threat actors, so tech companies must make an extra effort to protect their M&A process,” says Keating.

Hunting for threats in a target’s business relationships may well be the bigger challenge. Many executives are only now realizing the need for forensic analysis to determine whether a target company’s network has been hacked. But they must go further. “We’re working to educate companies to understand that, through their business relationships, they may be unwittingly and unknowingly allowing access to their systems to people who are looking to steal their IP,” explains Keating.

EY professionals can help M&A buyers explore whether there are potential cyber threats lurking within the extended layers of a given acquisition target’s business relationships. “We can analyze a target’s ownership structure, management team, joint ventures and other business relationships to determine whether there are indicators that may lead back to a nation-state, organized crime or hacktivist who is trying to find a way to get into your corporate network,” says Keating.

**Conclusion: proactively assess your cyber economic business risk**

At all times – but especially during an M&A process – technology companies should be thinking broadly about what EY calls “cyber economic business risk” (not only about defending their IT infrastructure). Cyber economic business risk embraces an organization’s strategic imperatives and broader set of business relationships and performs analyses to anticipate any economic, geopolitical or hacktivist threats that may exploit those relationships to steal your organization’s valuable IP.

“In this new environment, all companies must look way beyond their IT infrastructure to fully understand their cyber risk.”

Doree Keating  
Transaction Diligence  
Transaction Advisory Services  
Ernst & Young LLP
Questions to consider:

- Who has a vested interest in the success of our competitors?
- Who might profit from our IP?
- What hacktivists might have ideological differences with any positions our company has taken?
- How can we identify if cybercriminals have compromised our products?
- Have we investigated the extended business relationships of our M&A targets thoroughly enough from a cybersecurity perspective?
- How thoroughly have we assessed our overall cyber economic business risk?

“M&A is one of the few times where all functional areas of an organization get together to understand and assess risk. With that, there’s a large amount of documentation going back and forth between the companies. That activity creates an extremely attractive opportunity for cyber threat actors, so tech companies must make an extra effort to protect their M&A process.”

Doree Keating
Transaction Diligence
Transaction Advisory Services
Ernst & Young LLP
Find out more

Multifaceted security: preparing for cyber offense is part of a series of top-of-mind executive briefs providing separate deep-dive analyses of four disruptive technology transformation themes: stack to solution, hunting for hidden gems, in the crosshairs and multifaceted security.

For more information, or to discuss the diagnostic tools EY has developed to show how these themes might affect your own organization, contact Jeff Liu, at +1 415 894 8817 or jeffrey.liu@ey.com, Doree Keating, at +1 703 747 1327 or doree.keating@ey.com, or any of the contacts below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology sector contacts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pat Hyek, Global Technology Industry Leader</td>
<td>+1 408 947 5608</td>
<td><a href="mailto:pat.hyek@ey.com">pat.hyek@ey.com</a></td>
</tr>
<tr>
<td>Jeff Liu, Global Technology Industry Leader</td>
<td>+1 415 894 8817</td>
<td><a href="mailto:jeffrey.liu@ey.com">jeffrey.liu@ey.com</a></td>
</tr>
<tr>
<td>Winston Chung, Global Technology Sector Team</td>
<td>+1 415 984 7075</td>
<td><a href="mailto:winston.chung@ey.com">winston.chung@ey.com</a></td>
</tr>
<tr>
<td>Channing Flynn, Global Technology Industry Leader</td>
<td>+1 408 947 5435</td>
<td><a href="mailto:channing.flynn@ey.com">channing.flynn@ey.com</a></td>
</tr>
<tr>
<td>Dave Padmos, Global Technology Industry Leader</td>
<td>+1 206 654 6314</td>
<td><a href="mailto:dave.padmos@ey.com">dave.padmos@ey.com</a></td>
</tr>
<tr>
<td>Guy Wanger, Global Technology Industry Leader</td>
<td>+1 650 802 4687</td>
<td><a href="mailto:guy.wanger@ey.com">guy.wanger@ey.com</a></td>
</tr>
<tr>
<td><strong>Transaction Advisory Services (TAS) technology contacts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranjan Biswas, India</td>
<td>+91 806 727 5131</td>
<td><a href="mailto:ranjan.biswas@in.ey.com">ranjan.biswas@in.ey.com</a></td>
</tr>
<tr>
<td>Tim Dutterer, Co-Leader Technology, Parthenon-EY</td>
<td>+1 415 264 8442</td>
<td><a href="mailto:tim.dutterer@parthenon.ey.com">tim.dutterer@parthenon.ey.com</a></td>
</tr>
<tr>
<td>Staffan Ekström, Global Telecoms Leader – Transactions and TMT Leader, Nordics</td>
<td>+46 8 520 593 90</td>
<td><a href="mailto:staffan.ekstrom@se.ey.com">staffan.ekstrom@se.ey.com</a></td>
</tr>
<tr>
<td>David Hedley, US Technology M&amp;A Leader</td>
<td>+1 415 984 7128</td>
<td><a href="mailto:david.hedley@ey.com">david.hedley@ey.com</a></td>
</tr>
<tr>
<td>Neil Hutt, United Kingdom</td>
<td>+44 1189 281535</td>
<td><a href="mailto:nhutt@uk.ey.com">nhutt@uk.ey.com</a></td>
</tr>
<tr>
<td>Ben Kwan, TAS and TMT Market Segment Leader, Greater China</td>
<td>+852 2849 9223</td>
<td><a href="mailto:ben.kwan@hk.ey.com">ben.kwan@hk.ey.com</a></td>
</tr>
<tr>
<td>Simon Pearson, United Kingdom</td>
<td>+44 20 7951 0418</td>
<td><a href="mailto:spearsoneuk@ey.com">spearsoneuk@ey.com</a></td>
</tr>
<tr>
<td>Barak Ravid, Co-Leader Technology, Parthenon-EY</td>
<td>+1 415 894 8070</td>
<td><a href="mailto:barak.ravid@ey.com">barak.ravid@ey.com</a></td>
</tr>
<tr>
<td>Dr. Carsten F. Risch, Germany</td>
<td>+49 30 25471 21426</td>
<td><a href="mailto:carsten.risch@de.ey.com">carsten.risch@de.ey.com</a></td>
</tr>
<tr>
<td>Ken Smith, TAS Leader, Japan</td>
<td>+81 3 4582 6400</td>
<td><a href="mailto:kenneth.smith@jp.ey.com">kenneth.smith@jp.ey.com</a></td>
</tr>
</tbody>
</table>