GOHIO

Lessons Never Learned
A way through the valley

October 2017  |  Joel Fulton
“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era… we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses… account for the largest portion of economic and industrial information lost by US corporations.

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations… and are insulated form risks of internationally embarrassing incidents.

“The almost obsessive persistence of serious penetrators is astonishing.”

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.

“Our red teams do get into most of the networks we target.

“We’ve had market failure when it comes to cybersecurity. Security doesn’t come out of voluntary actions and market forces.

“Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.
“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era… we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.” - 1996

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.” - 1979

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.” - 1981

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses… account for the largest portion of economic and industrial information lost by US corporations.” - 1995

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations… and are insulated form risks of internationally embarrassing incidents.” - 1988

“The almost obsessive persistence of serious penetrators is astonishing.” - 1988

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.” - 2009

“Our red teams do get into most of the networks we target.” - 2008

“We’ve had market failure when it comes to cybersecurity. Security doesn’t come out of voluntary actions and market forces.” - 2012

“Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.” - 2010

“Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection.” - 2010
“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era. We’re not sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.”

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.”

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.”

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses… account for the largest portion of economic and industrial information lost by US corporations.”

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations… and are insulated from risks of internationally embarrassing incidents.”

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.”

“Our red teams do get into most of the networks we target.”

“We’ve had market failure when it comes to cybersecurity. Security doesn’t come out of voluntary actions and market forces.”

“Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.”

“Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets.”

“The Advanced Persistent Threats successfully evade anti-virus, network intrusion detection, and other best practices.”
Starting motivation

Where most people quit

Where the payoff is
### Strategy on a napkin

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Strategy on a napkin

<table>
<thead>
<tr>
<th></th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>X</td>
<td>X</td>
<td>!</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Strategy on a napkin

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Order of operations

Protect

Identify

Detect

Respond

Recover
Order of operations

- Protect
- Identify
- Detect
- Recover
- Respond

B+
Order of operations
Security Efficacy Consequences

Identify: 0 70 100
Protect: 0 49 0
Respond: 0 39 0
Recover: 0 39 0

<F>
Security Efficacy Consequences
Thank you

Joel Fulton, PhD
CISO
jfulton@splunk.com