



Lookingglass
Vision. Awareness. Intelligence.

Using Threat Intelligence to
Understand Cyber Ecosystem Risk

Derek Gabbard, CEO, Lookingglass
GFIRST 2011

Overview

- Learning Objectives
 - Define the characteristics of a cyber ecosystem, to include partners, providers, customers, etc.
 - Describe cyber threat intelligence and the basic tenets required to achieve it
 - Define the important data sets to be collected and enrichment processes for that data to give threat intelligence
 - Describe the actions which can be undertaken by security and operations teams once threat intelligence has been achieved

Cyber Ecosystem

- Evolution of the cyber ‘ecosystem’ (aka ‘extended enterprise’)
 - ‘Managed Services’ relationships
 - Partnerships
 - Other providers
 - M&A activities
 - 3rd party providers/suppliers
- Years ago, network traffic left the enterprise and was ‘outside the view’ of the enterprise players

Fundamental Risk Management Axiom:

Risks of which you are unaware and do not mitigate are risks you inherently accept.



Internet Ecosystems/Supply Chains

- **Case in point: Marketing Services Company X**
 - Enterprises outsource email marketing services to a third party email marketing organization
 - Spear phishers target Marketing Services Company X and successfully compromise systems there with malware which disabled anti-virus software, installed a Trojan keylogger called iStealer (which was used to steal passwords), and install an administration tool called CyberGate (which is used to gain complete remote control of compromised systems)
 - After credentials are stolen by phishers, massive exfiltration of sensitive information occurs



Cleanup - Ecosystem 'Breach'

Dear Valued Best Buy Customer,

On March 31, we were informed by [REDACTED], a company we use to send emails to our customers, that files containing the email addresses of some Best Buy customers were accessed without authorization.

We have been assured by [REDACTED] that the only information that may have been obtained was your email address and that the accessed files did not include any other information. A rigorous assessment by [REDACTED] determined that no other information is at risk. We are actively investigating to confirm this.

For your security, however, we wanted to call this matter to your attention. We ask that you remain alert to any unusual or suspicious emails. As our experts at Geek Squad would tell you, be very cautious when opening links or attachments from unknown senders.

In keeping with best industry security practices, Best Buy will never ask you to provide or confirm any information, including credit card numbers, unless you are on our secure e-commerce site, www.bestbuy.com. If you receive an email asking for personal information, delete it. It did not come from Best Buy.

Our service provider has reported this incident to the appropriate authorities.

We regret this has taken place and for any inconvenience this may have caused you. We take your privacy very seriously, and we will continue to work diligently to protect your personal information. For more information on keeping your data safe, please visit:

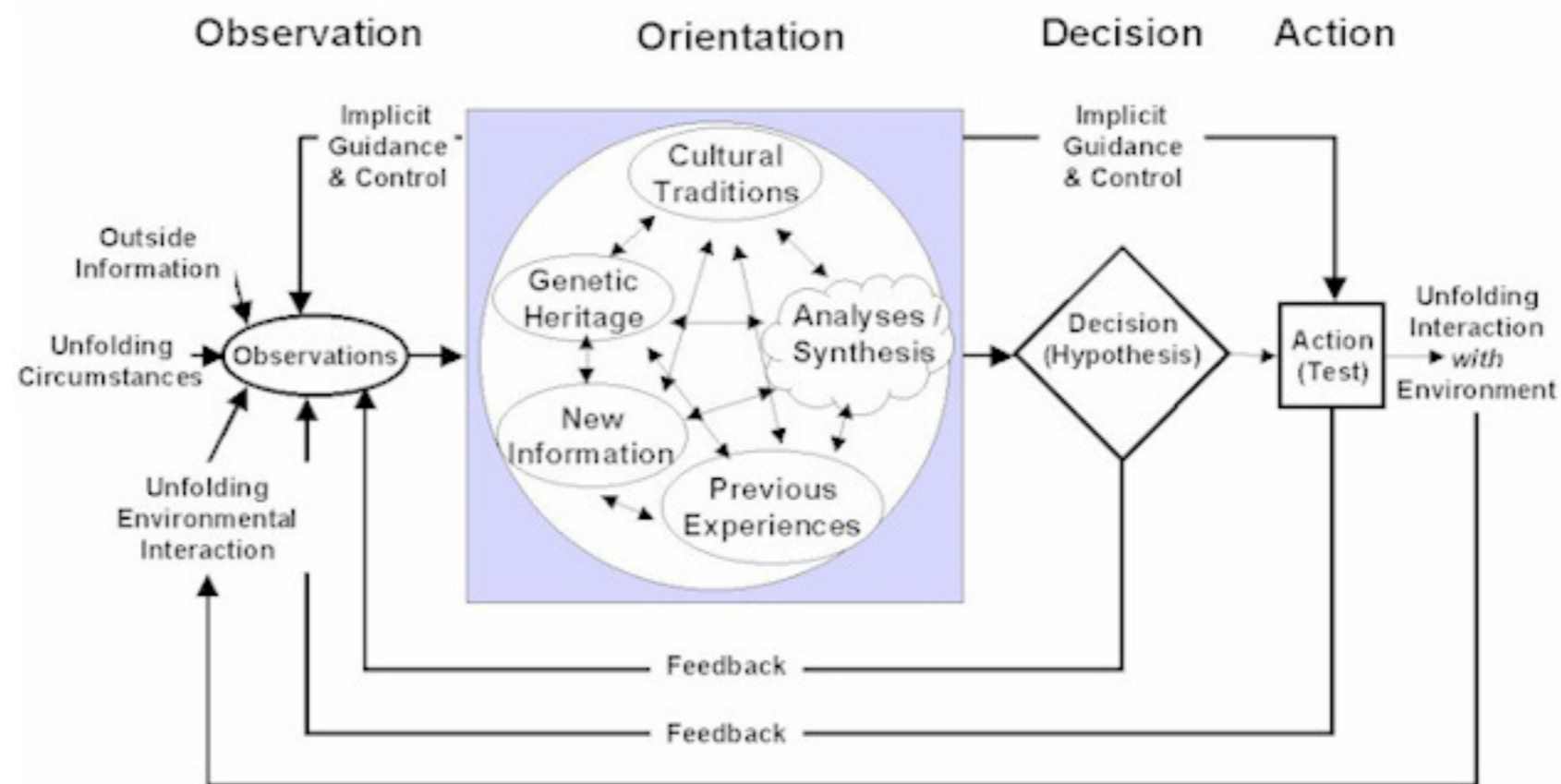
<http://www.geeksquad.com/do-it-yourself/tech-tip/six-steps-to-keeping-your-data-safe.aspx>.

Sincerely,

Executive Vice President & Chief Marketing Officer
Best Buy

Cyber Threat Intelligence

- Process for gathering and fusing appropriate data sets, enriching those sets to provide actionable information, and acting on that information
- Useful military model here: the OODA loop





Basic Questions for Creating Cyber Threat Intelligence - Observe

- Observe
 - What organizations are in our ecosystem?
 - How do those organizations serve us?
 - What are the issues which would cause concern when considering the security stance of that organization?
 - How do we get the appropriate data to allow us to gain the appropriate visibility into their security posture?

- Answers
 - List of 3rd parties
 - List of VPN partners, etc.



Basic Questions for Creating Cyber Threat Intelligence - Orient

- **Orient**
 - How do we consume the data we would be collecting?
 - How do we enrich the data we would be collecting?
 - When do we know if we need more data?
 - How do we know if our data is good?
- **Answers**
 - Global data sets which offer visibility into the status of the networks in question
 - Global routing and naming data sets to determine 'cleanliness' of target networks



Basic Questions for Creating Cyber Threat Intelligence - Decide

- **Decide**

- What are our options once we have observed problems in our ecosystem which are beyond our control?
- How do we inform appropriate players of those problems?
- How will a response impact our relationship with the organization in question?
- How does the problem in question pose risk to our organization?
- Is there a means to control that?

- **Answers**

- Analyze network access/connectivity with risky networks
- Involve business operations to ratify organizational decisions



Basic Questions for Creating Cyber Threat Intelligence - Act

- **Act**

- Instantiate activities (not really 'response' as this could be pro-active)
- Report to all organizations involved
- Share info!

- **Answers**

- Turn off access
- Implement SLA activities
- Fine/sue



‘Try This at Home’

- Define ecosystem players for your organization
 - Limit to smaller number to start - 20 or less
- Set up monitors for problematic activity within their networks and name space
- Take reports on activity to management and/or business units which use services offered by ecosystem members and show them the risks
- Offer response options which allow the business to operate but minimize risk
- Get promoted.



Lookingglass
Vision. Awareness. Intelligence.

Need help?

Derek Gabbard, CEO, Lookingglass

dgabbard@lgscout.com



References

“DHS shares vision of a healthy cyber ecosystem” Meg Beasley , Federal News Radio, July 8 2010 (<http://www.federalnewsradio.com/?nid=35&sid=1998512>)

“What’s in your extended enterprise?” Rod Rasmussen, SecurityWeek, 25 Aug 2010, (<http://www.securityweek.com/whats-your-extended-enterprise>)

“Cyber-vulnerabilities in the 'extended enterprise'” Louis Chunovic, Government Security News, Sept 23 2009

“Epsilon Breach: Hack of the Century?” Darlene Storm, Computer World, April 4 2011. (http://blogs.computerworld.com/18079/epsilon_breach_hack_of_the_century)