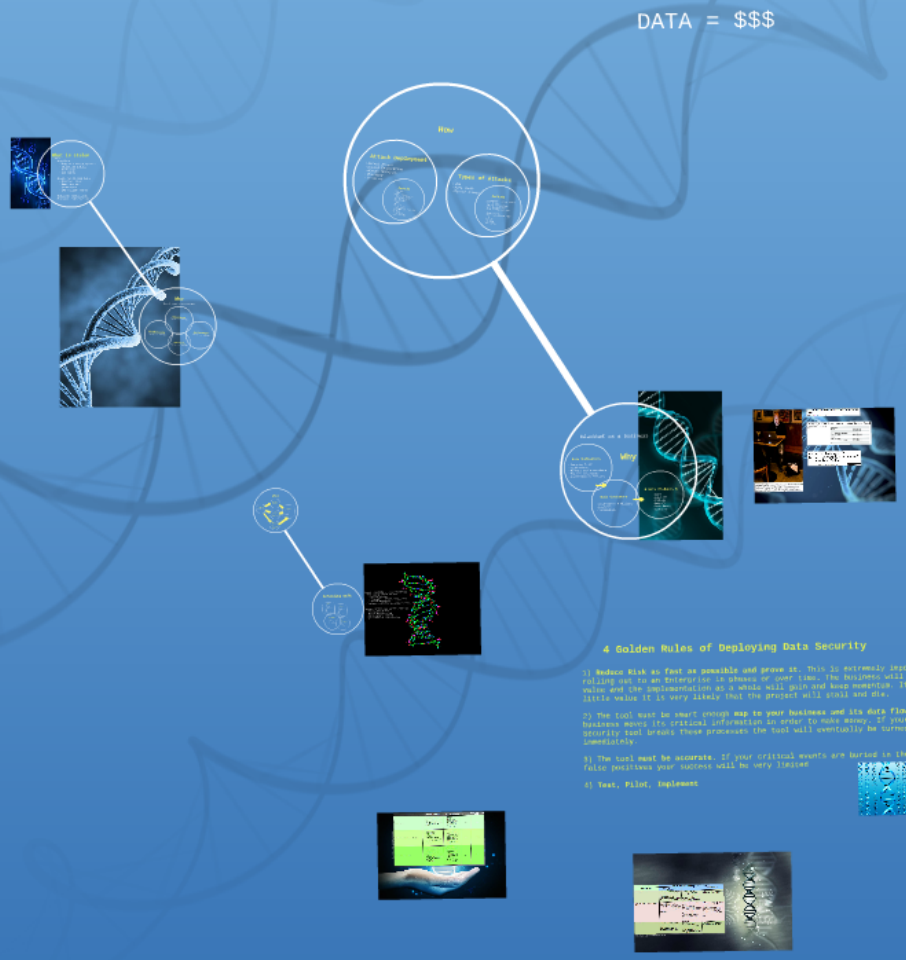
The DNA of Data Theft

WHAT | WHO | WHY | HOW | WHEN

Charles Sirois
Chief Security and Strategy Officer
Assurance Data Inc



The DNA of Data Theft

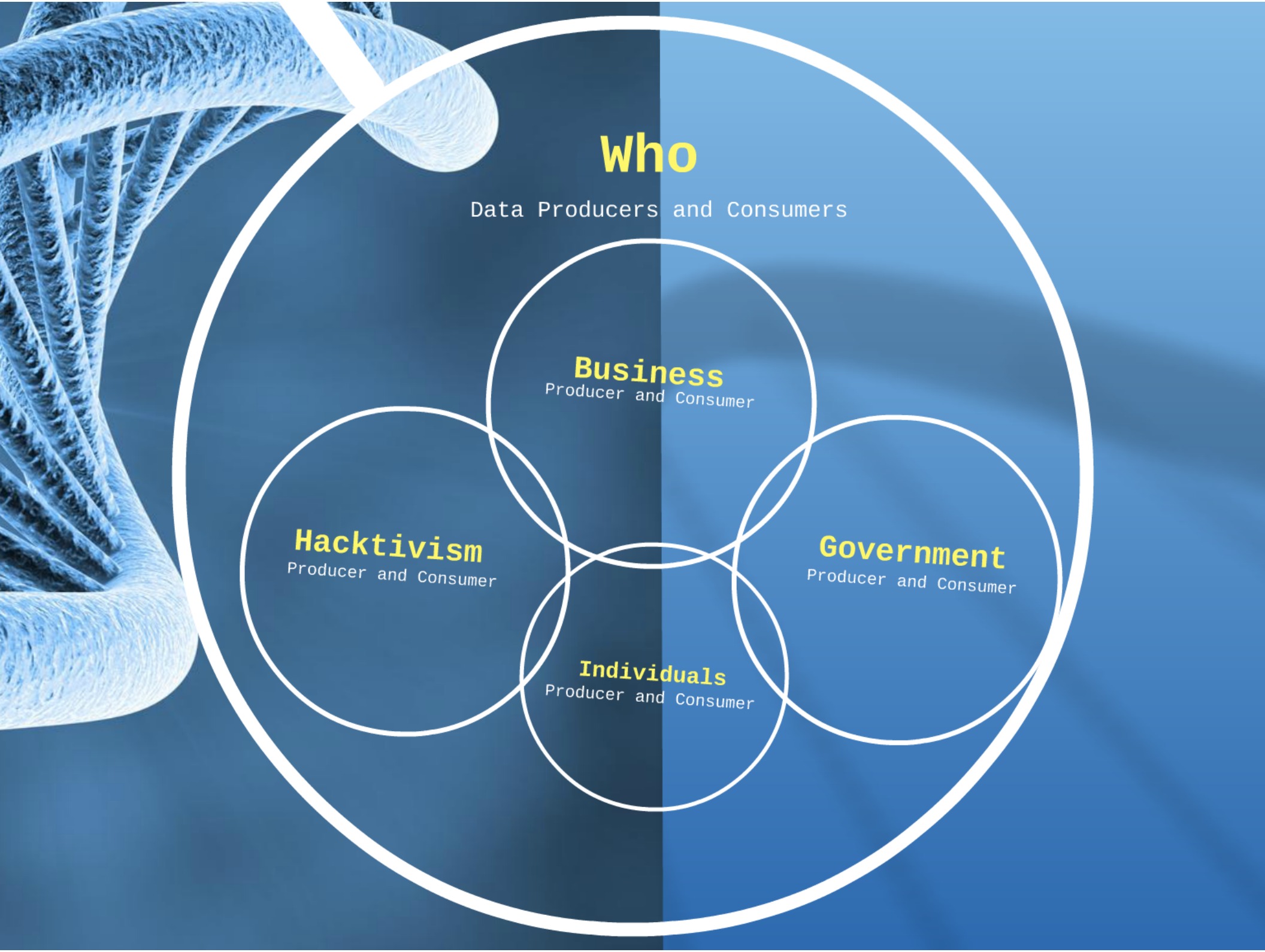
WHAT | WHO | WHY | HOW | WHEN

Charles Sirois
Chief Security and Strategy Officer
Assurance Data Inc

What is stolen

Data

- Big Data
  - Asks for participation
  - Collected public knowledge
  - Big money
- Black Market Big Data
  - Blurred lines
  - Does not ask permission
  - Even bigger money
- Business Operations
- Personal Information


Who
Data Producers and Consumers
Business
Producer and Consumer
Hacktivism
Producer and Consumer
Government
Producer and Consumer
Individuals
Producer and Consumer

Blackhat as a business

Why

Data Collectors

- Security Teams
- Hacktivists
- Hackers and Researchers
- Private businesses
- Governments & Military

Data Customers

- Governments & Military
- Business
- Individuals

$ Data Products $

- DATA
- Exploits
- Zombies
- Botnets
- Back Doors
- Identity

High-end exploit broker "the Grugq" at a Bangkok bar. The bag of cash at his feet is for one of his exploit developers. (Photo credit: Christopher Wise/Redux)

Security Firm Outbids Apple With $500,000 Bounty for iOS Flaws

By eWEEK Staff | Posted 2016-08-12 Print

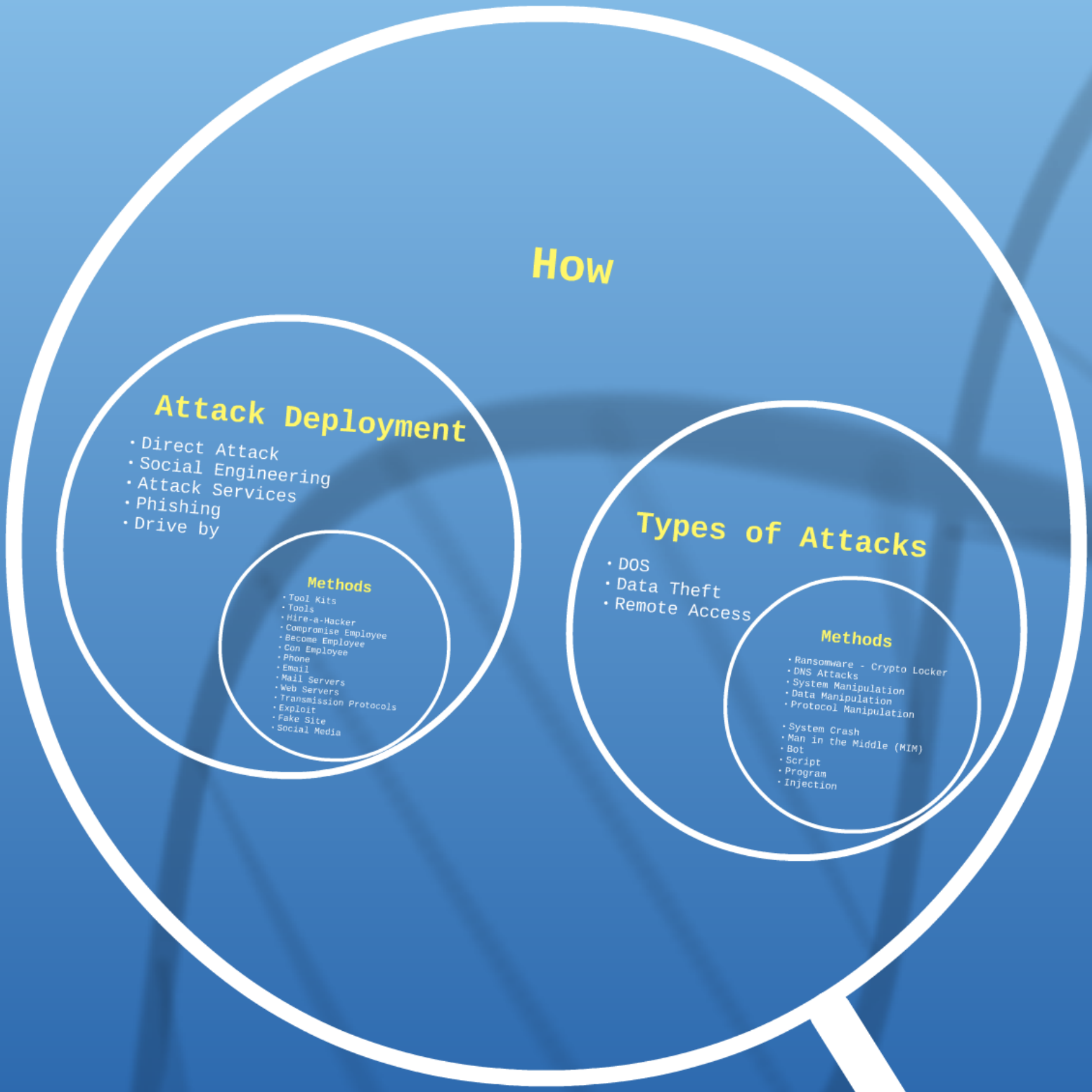
Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Broker Outbids Apple Bug Bounty Program by Hundreds of Thousands of Dollars

by Robert Hackett @rhhackett AUGUST 10, 2016, 5:16 PM EDT

FORTUNE


How
Attack Deployment
Direct Attack
Social Engineering
Attack Services
Phishing
Drive by
Methods
Tool Kits
Tools
Hire-a-Hacker
Compromise Employee
Become Employee
Con Employee
Phone
Email
Mail Servers
Web Servers
Transmission Protocols
Exploit
Fake Site
Social Media
Types of Attacks
DOS
Data Theft
Remote Access
Methods
Ransomware - Crypto Locker
DNS Attacks
System Manipulation
Data Manipulation
Protocol Manipulation
System Crash
Man in the Middle (MIM)
Bot
Script
Program
Injection

Types of Attacks

- DOS
- Data Theft
- Remote Access

Methods

- Ransomware - Crypto Locker
- DNS Attacks
- System Manipulation
- Data Manipulation
- Protocol Manipulation

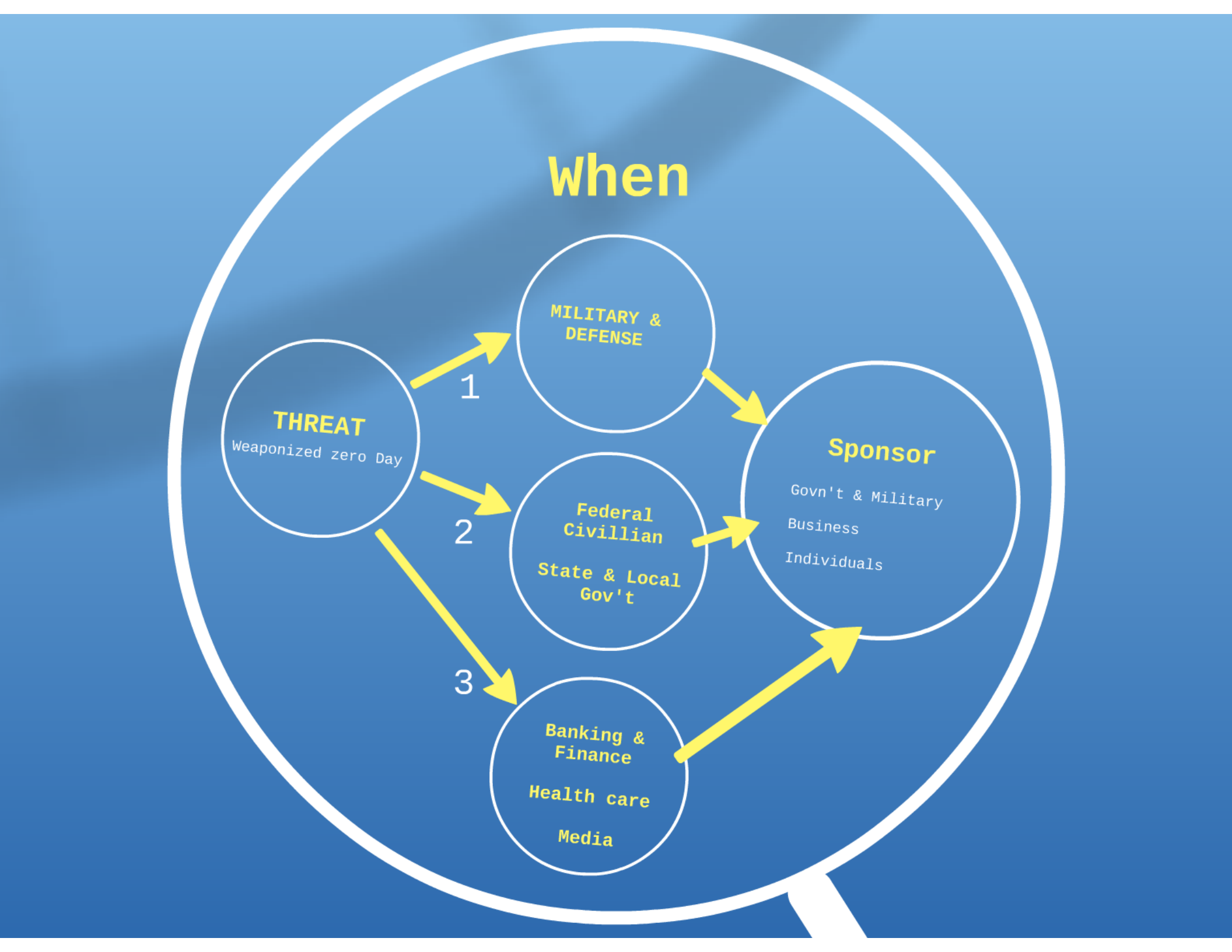
- System Crash
- Man in the Middle (MIM)
- Bot
- Script
- Program
- Injection

Attack Deployment

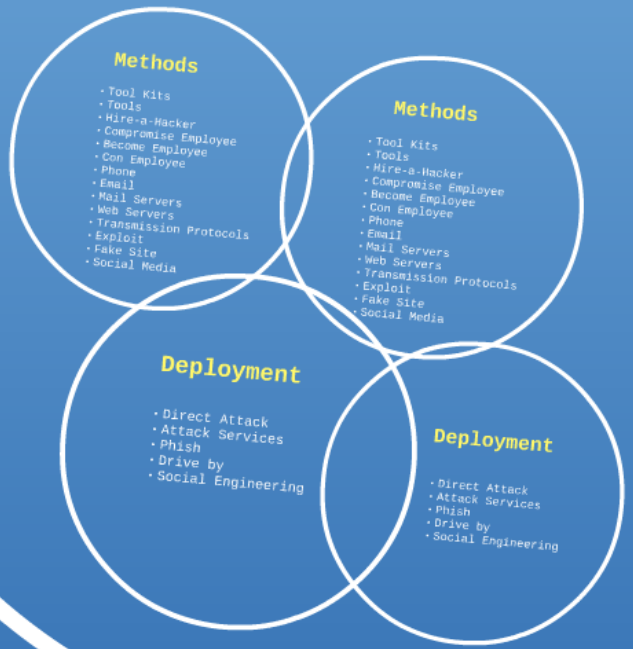
- Direct Attack
- Social Engineering
- Attack Services
- Phishing
- Drive by

Methods

- Tool Kits
- Tools
- Hire-a-Hacker
- Compromise Employee
- Become Employee
- Con Employee
- Phone
- Email
- Mail Servers
- Web Servers
- Transmission Protocols
- Exploit
- Fake Site
- Social Media


When
THREAT
Weaponized zero Day
1
MILITARY & DEFENSE
2
Federal Civillian
State & Local Gov't
3
Banking & Finance
Health care
Media
Sponsor
Govn't & Military
Business
Individuals

Defending DATA



Global knowledge of threat landscape

- Minimizing attack surface
  - System updates
  - Transport/ protocol Monitoring
  - System monitoring
- Business community knowledge sharing

Business model data centric controls

- Data flow mapping
- Data flow monitoring
- Securing Data storage
- Securing Data Transmissions

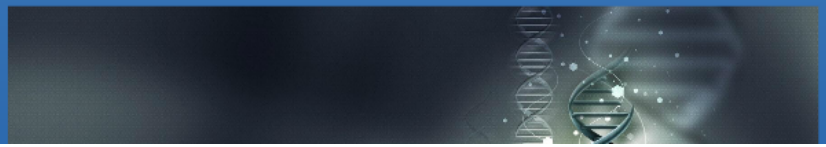
4 Golden Rules of Deploying Data Security

1) **Reduce Risk as fast as possible and prove it**. This is extremely important when rolling out to an Enterprise in phases or over time. The business will find fast value and the implementation as a whole will gain and keep momentum. If you show little value it is very likely that the project will stall and die.

2) The tool must be smart enough **map to your business and its data flow**. Your business moves its critical information in order to make money. If your Data Security tool breaks these processes the tool will eventually be turned off, if not immediately.

3) The tool **must be accurate**. If your critical events are buried in thousands of false positives your success will be very limited

4) **Test, Pilot, Implement**

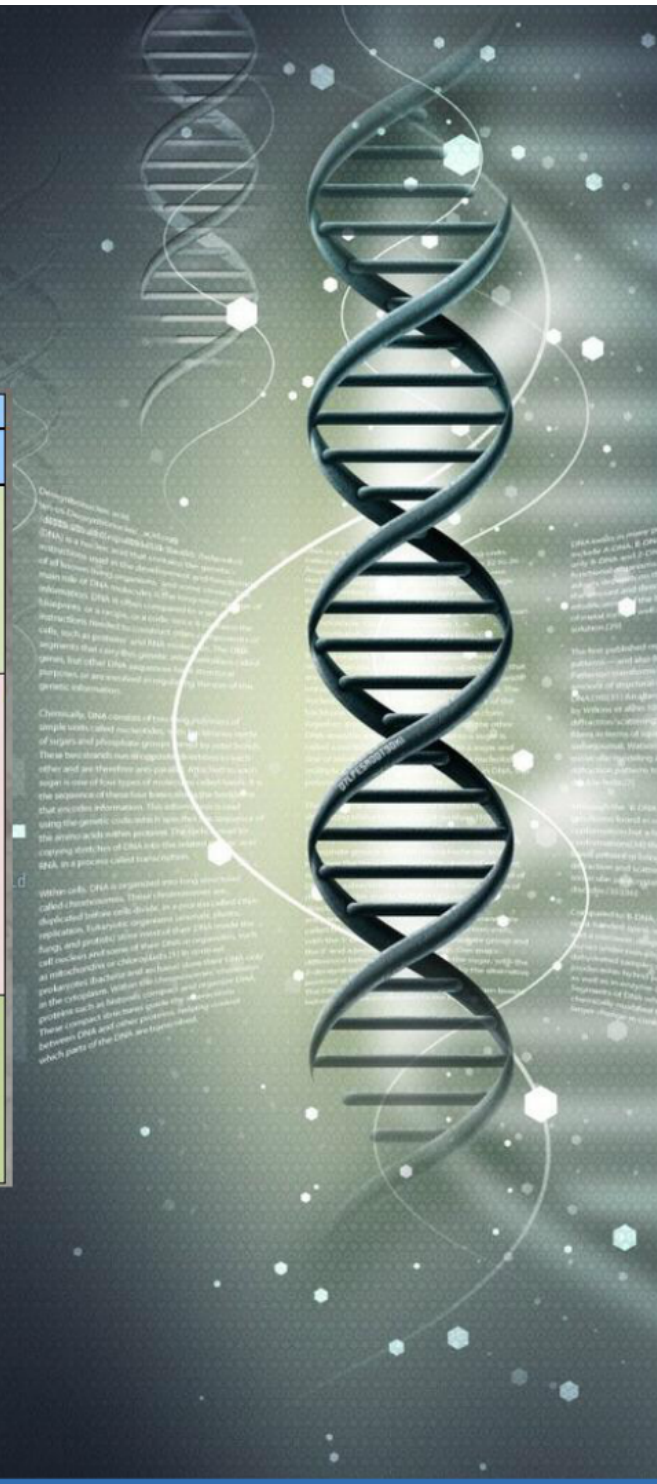


Maturity	Methods [of Data Detection]	Policy to Business Mapping	Risk Reduction	Typical Accuracy/ False positive
Phase I: Monitoring	• File Properties [type, size, age] • Key words, Patterns, dictionaries • OCR (Optical Character Recognition) or a more modern term GTA (Graphical Text Analysis)	• Discovering business processes • Early blocking of damaging destinations • Data use discovery • Data transfer method Discovery • Drip DLP monitoring	20%	80/20
Phase II: Notifications & End user Education	• Regular Expressions • Lexical analysis • Statistical analysis • File Tagging • OCR (Optical Character Recognition) or a more modern term GTA (Graphical Text Analysis)	• end user notifications • Continued blocking of damaging destinations • Destination Awareness • Data Source Discovery • Data use discovery • Data transfer method Control • Intro to "Drip DLP" control	50%	90/10
Phase III: Blocking & Control	• File hashing/ Fingerprinting • Database record hashing/ fingerprinting • Multi-accuracy/ blended policies • OCR (Optical Character Recognition) or a more modern term GTA (Graphical Text Analysis) • Machine learning	• End user Education • Blocking of bad business processes • Source and Destination Control • Data Destination Control • Data transfer method control • Data use control • Data Source Control • Advanced "Drip DLP" control	80%+	95+/5-

Source: DataLeakTest.com

Where to start	Keys to Success [the golden rules of Data Security]		
Methods/Channels	**Policy Mapping to Business Processes**	**Data Security Tool Accuracy**	**Risk Reduction/ROI**
Data-In-Motion (DIM)	Can the product fit to your business without interrupting good business transactions while protecting the data and preventing misuse? **Required before phases II and III of the Data Security Deployment/ maturity Model.**	Essential for mapping to the business and catching real events. **Policies are ratcheted down for accuracy in phase I before moving into phase II of the Data Security Deployment/ Maturity Model**	Phases II and III **of the Data Security Deployment/ Maturity Model**
Data-At-Rest (DAR) [*hint **DON'T START HERE**]'	Easy to find the data but you must engage the business to figure out why the data is there. The business processes are nearly impossible to uncover without extensive business involvement.	Easy to find data types with predefined policies and easy to make your own. Some companies think that the results from a DAR scan will help then define data but often have trouble sorting through the results they get from a DAR scan… requiring business involvement for clarity. Most find this process very time consuming.	**Shelf-ware alert!** ROI is very low and rarely moves out of Data Security phase I. Companies that lead with DAR often find Data Security results ineffective at demonstrating ROI. This makes it difficult to justify applying resources to DIM or DIU. Phase III is rarely accomplished with DAR.
Data-In-Use (DIU)	Insight into how data is used by applications and when not in the office. **Required before phases II and III of the Data Security Deployment/ Maturity model.**	Essential for mapping to the business and catching real events. **Policies are ratcheted down for accuracy in phase I before moving into phase II of the Data Security Deployment/ Maturity Model**	Phases II and III of the **Data Security Deployment/ Maturity Model**

Source: DataLeakTest.com




DATA = $$$