InteliSecure

THE BUSINESS CASE FOR IMPLEMENTING DLP

DATE: 10/9/2014

Agenda

InteliSecure

- Real World DLP Successes
- Identifying “Your” Critical Assets
- Leveraging Data Loss Prevention to Monitor Critical Assets – DLP Policy Governance
- Security Humanistics
- Measuring Success – Review of KPI’s, Reporting and Metrics for CAPP & DLP Programs

Five Companies Developing New Cancer Drugs

Wed, Oct 8, 2014, 6:26pm EDT - US Markets are closed

5 Companies Developing New Cancer Drugs

benzinga By Tabitha Jean Naylor
August 19, 2014 1:20 PM

The search for a cure for cancer has consumed the public discourse around the world and the United States for as long as one can remember.

The Five Companies

- OncoSec Medical (OTC: ONCS)
- ImmunoCellular Therapeutics (NYSE: IMUC)
- Celldex Therapeutics (NASDAQ: CLDX)
- Northwest Biotherapeutics (NASDAQ: NWBO)
- Inovio Pharmaceuticals (NYSE: INO)

- **Combined R&D for 2013 = approximately $136 million**

Inovio – Focused on Ebola Today

InteliSecure

Inovio CEO: New Ebola vaccine effective in animals

Bruno J. Navarro | @Bruno_J_Navarro
Wednesday, 1 Oct 2014 | 6:46 PM ET

CNBC

One synthetic **Ebola** vaccine in development has shown preliminary success in beating back the deadly virus, **Inovio Pharmaceuticals** CEO and President Joseph Kim said Wednesday.

"We were able to see 100 percent protection in animal models, in two separate animal species, after these animals were vaccinated with Inovio's Ebola vaccine," he said, adding that the subjects avoided illness and death. The results, he added, were published in a peer-reviewed medical journal late last year.

Inovio – Income Statement

InteliSecure

Income Statement

Get Income Statement for: GO

View: **Annual Data** | Quarterly Data

All numbers in thousands

Period Ending	Dec 31, 2013	Dec 31, 2012	Dec 31, 2011
Total Revenue	**13,467**	**4,119**	**9,795**
Cost of Revenue	-	-	-
Gross Profit	**13,467**	**4,119**	**9,795**
Operating Expenses			
Research Development	21,369	17,985	20,032
Selling General and Administrative	13,643	10,778	11,989
Non Recurring	-	-	-
Others	-	-	-
Total Operating Expenses	-	-	-
Operating Income or Loss	**(19,544)**	**(23,494)**	**(21,639)**
Income from Continuing Operations			
Total Other Income/Expenses Net	(44,539)	4,932	6,921
Earnings Before Interest And Taxes	(64,084)	(18,562)	(14,717)
Interest Expense	-	-	-
Income Before Tax	(64,084)	(18,562)	(14,717)
Income Tax Expense	-	-	-
Minority Interest	55	44	51
Net Income From Continuing Ops	(64,028)	(18,518)	(14,666)
Non-recurring Events			
Discontinued Operations	-	-	-
Extraordinary Items	-	-	-
Effect Of Accounting Changes	-	-	-
Other Items	-	-	-
Net Income	**(66,028)**	**(19,669)**	**(15,253)**
Preferred Stock And Other Adjustments	-	-	-
Net Income Applicable To Common Shares	**(66,028)**	**(19,669)**	**(15,253)**

The Buisness Case for DLP and CAPP at Inovio

InteliSecure

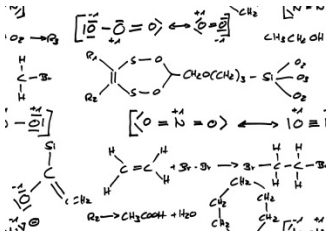
- Developing possible game-changing drugs for cancer, HPV and Ebola, among others
- What are the critical assets?
- How can DLP help protect this organization?
- How would you position DLP and CAPP to executives?

InteliSecure

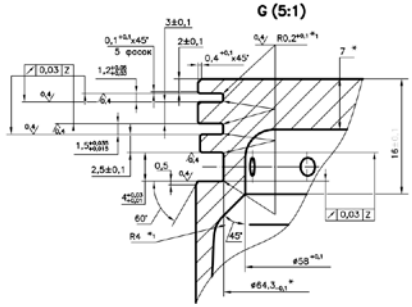
Identifying Critical Assets

What is a Critical Asset?

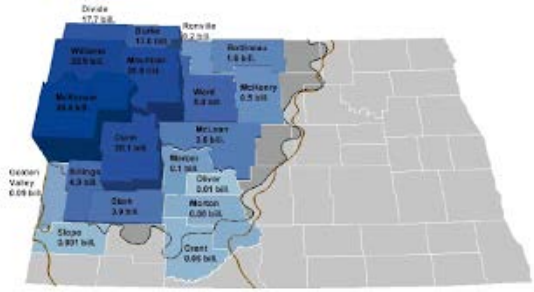
A critical asset is a piece of information or data that, if compromised or leaked could cause irreparable harm to an organization.



Product Formulas



Product Designs



Research Information

PII

Transaction Information

Critical Asset Protection Program Approach

Critical Asset Lifecycle Mapping

InteliSecure

Critical Asset Creation

The point in time when the asset is created. This could be the first swipe of a credit card, the initial lines of code for a new application or the acquisition of a new VM Cluster. Today, asset creation can be the product of multiple groups or systems.

Critical Asset Storage

Once the asset has been created the asset is stored. For intangible assets this may be in RAM, on a hard disk, NAS, SharePoint or other types of data storage. Tangible assets like servers, routers or laptops may be racked in a datacenter, placed in a remote office closet or placed on a home office desk.

Critical Asset Use

Protecting the critical assets becomes a more manageable endeavor by mapping the authorized usage characteristics of the assets within the CAPP scope, and then applying the optimal combination of people, process and technology.

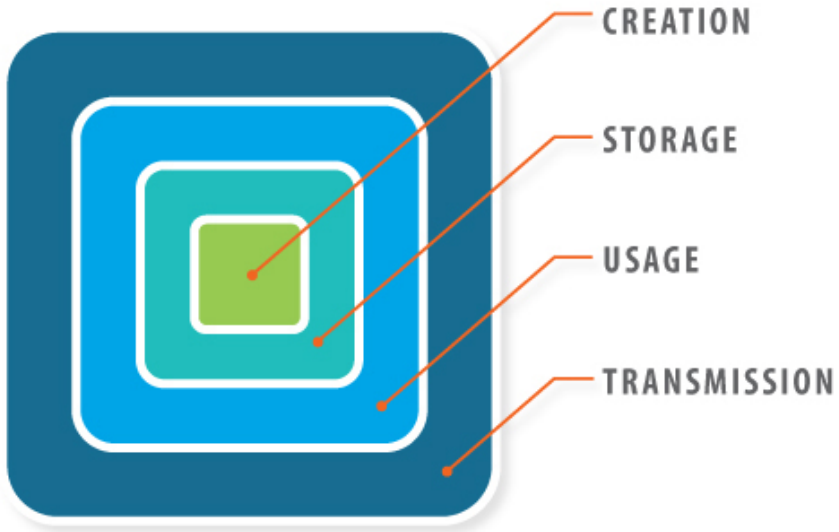
Critical Asset Transmission

The transmission threat vector is utilized for authorized operations. Assessing how critical asset information is shared within and outside the organization provides key insight to the required protection mechanisms necessary to protect against inadvertent or malicious asset exposure.

Critical Asset Protection Programs (CAPPs)

CAPPs clearly define what assets are deemed most important to an organization based on revenue, income, reputation and core operational impact.

CAPP scope defines the assets as well as the core attributes of those assets in regards creation, storage, usage and transmission.



3Cs Guide to CAPP Creation

InteliSecure

- Identify Content
  - Information contained within and the format of the asset
- Monitor Channels
  - Identify how critical assets move within and out of networks
- Target Community
  - Identify people and systems authorized to access specific data

Examples of the 3Cs

1. Engineering specifications
2. Manufacturing processes
3. Test Well Data
4. Fracking Formulas
5. Personnel Information

1. Email
2. Removable media
3. Large file transfers
4. Print/fax
5. FTP data
6. Data posted to the web

1. All employees
2. Engineering and purchasing
3. Approved vendors
4. Outside accounting firm
5. Research & Development

Leveraging Data Loss Prevention to Monitor Critical Assets – DLP Policy Governance

Identify Purpose for Monitoring

InteliSecure

Generally Acceptable Business Reasons Include:

- **Prevent industrial espionage**
- **Protect against unauthorized use, disclosure or transfer of PII**
- **Prevent or detect unauthorized utilization of employer's computer system for criminal activities & terrorism**
- Monitor & maximize employee productivity
- Monitor employee compliance with employer workplace policies
- Investigate complaints of employee misconduct
- Prevent or respond to unauthorized access to employer's computer systems
- Protect computer networks from becoming overloaded
- Help prepare employer's defense to lawsuits or administrative complaints
- Respond to discovery requests in litigation related to electronic evidence

Application Support & Integration

InteliSecure

- Primary System DLP Management =
  Human Resource / Expertise Requirements
- Integrated System Management =
  Cross Department Collaboration Processes
- Health Check & System Validation Management =
  System Resource Requirements
- Vendor Management =
  Primary and Integrated Technology Vendor Relationships

Policy & Rule Governance

InteliSecure

Who requests rules & policy requirements?

Are business owners engaged?

Who reviews rule requests?

Criteria for approved rule?

What's the process for converting a rule request into a policy?

Who's responsible for converting a rule into technical policy?

Do they have technical policy authoring expertise?

What is the formal policy development process?

First drafts rarely work as expected!

Is there a process to relay production policy metrics to stakeholders?

Workflow Development & Management

InteliSecure

Who develops & manages policy “buckets”?

False positive, inbound partner, outbound employee

Who defines thresholds that determine response rules for each “bucket”?

Are 10 SSNs a high, medium or low severity incident?

Who designs & sets the policy response triggers?

Malicious, Inadvertent, Suspicious, above threshold.

Triage response options:

- Human notification
- System notification (auto)
- Hybrid?

Who’s responsible for building alerts, alarms & notifications?

Has business been engaged on event management?

Who manages the DLP policy & rules repository?

Why recreate the wheel?

Incident Triage & Event Management

InteliSecure

Who reviews volume & yield of incidents & events?

What's the review frequency?

How are events/incidents routed?

Who owns the incident/event?

How does DLP fit in overall incident/event management process?

Can this be mapped to DLP system?

What metrics are developed to measure success of rules & related policy?

Who 's responsible for developing metrics?

Revision of rules based on quality of policy results.

Who manages policy optimization process?

How will integrated systems be tied together to yield valued info?

Secure mail, web gateway, GRC, SIEM

Business Analytics

InteliSecure

- Who drives report requirements? Requestors, Reviewers, others?
- Who develops reports?
- Do they have the expertise with 3rd party reporting tools?
- Are DLP system generated reports adequate?
- Are the metrics valuable & driving meaningful change?
- Report accuracy tied into QA process?

Security Humanistics

Data Loss Research

InteliSecure

- 88% of participants believe the risk of privileged user abuse will increase or stay the same in the next 12 – 24 months
- 64% of all data loss is caused by well meaning employees
- 50% of all employees leave with proprietary data
- 59% of companies don't have adequate intelligence or are unsure of attacks

Sources: "Cost of a Data Breach Report", Symantec and Ponemon Institute; "Privileged User Abuse & The Insider Threat, Ponemon Institute, May 2014

Security Humanistics

- Logs and reports do not reveal the whole story
- Correlation between technologies and incidents requires a human element
- Humanistics includes the people using information as well as those monitoring information

Measuring Success – Review of KPI's, Reporting and Metrics for CAPP & DLP Programs

Example DLP Program Benchmarks and Goals

InteliSecure

SHORT-TERM INIATIVES

- Policy enhancement project
- Expansion of network policies to enterprise
- Creation of sensitive document policy

LONG-TERM INIATIVES

- PCI-compliant DLP (Data Loss Prevention) environment
- Upgrade to Symantec DLP version 12.5
- Upgrade endpoint agents to Symantec DLP version 12.5

PROGRAM GOALS

- Continued policy expansion and accuracy tuning
- Business-driven adoption of DLP across enterprise, growth of program and policies
- Full monitoring of all users across Email and Endpoint channels

DLP Unauthorized Activity

InteliSecure

TOP OFFENDERS GENERATING UNATHORIZED ACTIVITY (1)

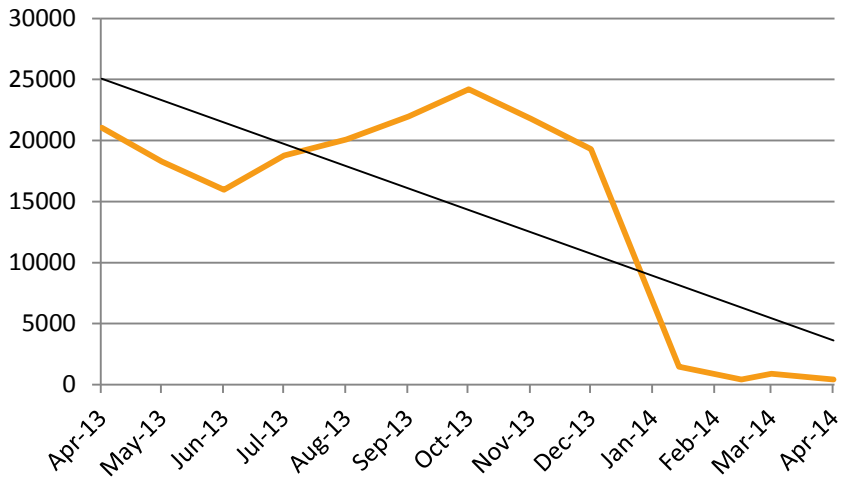
	Alias	Title	Department	Events Generated	Details
Network Prevent	TZJ4	Mortgage Loan Closer	Bank	31	31 incidents escalated to IRT
	TKQ5	Business Lender	Bank	23	23 unencrypted emails containing SSNs
	TTPG	External Associate	IT/Systems	24	24 unencrypted emails containing SSNs
Endpoint Prevent	RAF9	Intern	Finance	870	870 files transferred to an unauthorized device
	KP79	VP of Finance	Finance	602	602 files transferred to an unauthorized device
	IZXZ	Compliance Analyst	Legal	198	198 files transferred to an unauthorized device
	CISQ	Human Resources Manager	HR	105	Transfer of same 5 files recurring monthly from September 1- April 1

Overall Trending

InteliSecure

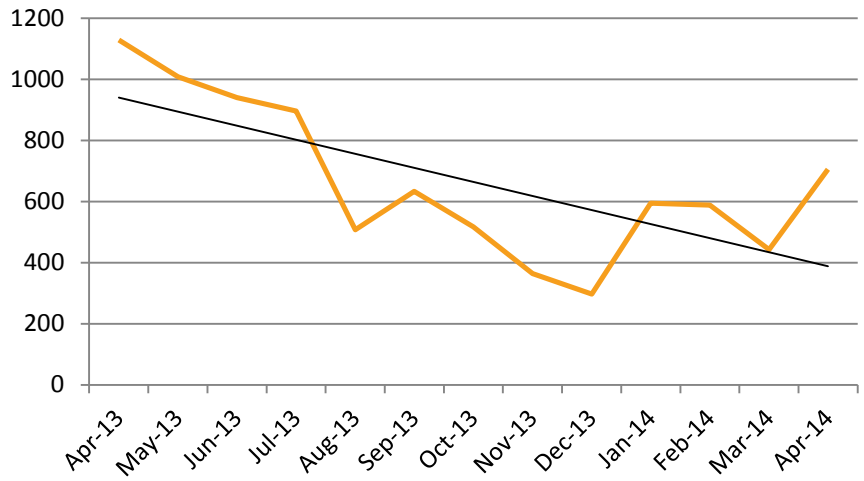
TRUE POSITIVE EVENTS 12-MONTH LOOKBACK (1)

Monthly Endpoint Events Since April 2013



- Successful policy tuning efforts are reflected in the December 2013 drop in total events

Monthly Network Events Since April 2013



- Event detection spikes as program ramped up and policies rolled out to full groups
- As user education and policy accuracy increases, events show a downward trend

(1) Network monitoring began in July 2012, while Endpoint began in March 2013

Questions?