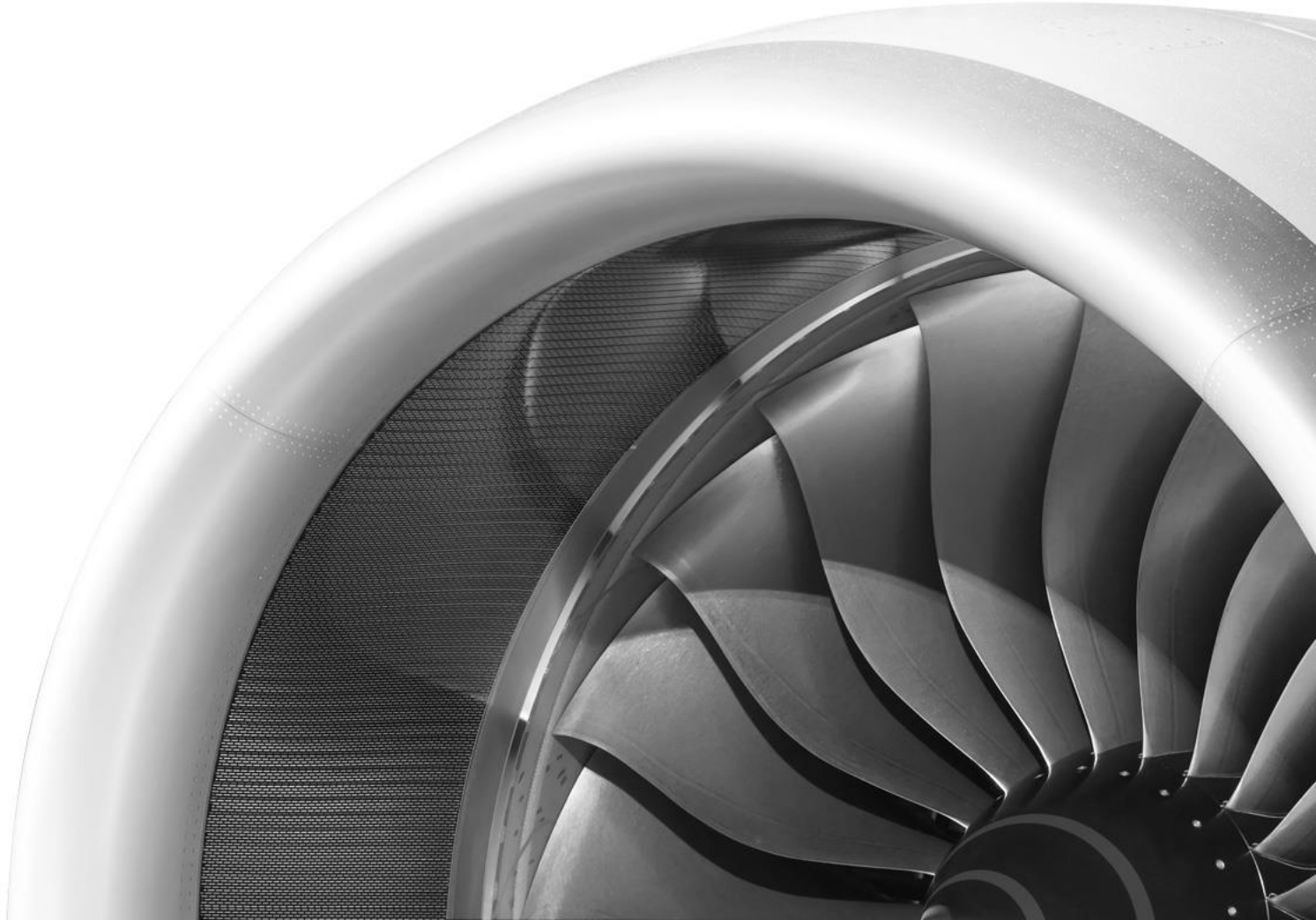
Data Loss Prevention

Edward Portolese – CIO

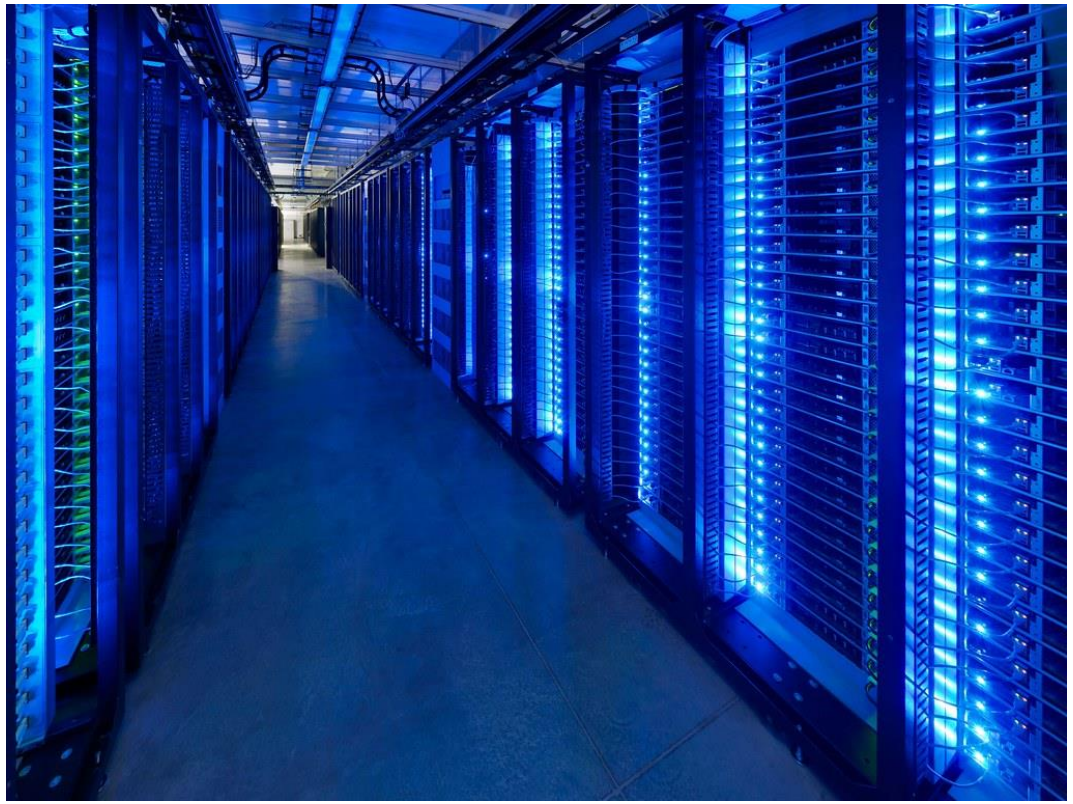
Ryan Shaw – CISO

HOWMET AEROSPACE



Agenda

- Introduction
  - Hi!
  - DLP / CASB 101
  - Why should you run a DLP program?
- What makes for a successful program?
- Tool and vendor selection considerations
  - Culture
  - Staffing
  - Privacy and Legal
  - Fit with other tools
- What you may find
  - Intellectual property misappropriation
  - Personal identifiable information loss
  - High risk business processes



HOWMET AEROSPACE

Introduction

Introduction – Ryan Shaw

- CISO – Howmet Aerospace
  - Formerly known as Arconic….
    - Formerly known as Alcoa…
- Directs Company global cyber security program
- Avid InfoSec nerd
- B.S in Computer Science and Info. Systems
- M.S from CMU in Information Security

DLP and CASB 101

What it is…

- Data Loss Prevention (DLP) **tools** are designed to aid and inform your data loss prevention **program**
- Cloud Access Security Brokers (CASB) are enforcement points between cloud providers and cloud consumers
  - Allow you to control cloud service behavior as if it were on-prem
- Incredible source of data that needs to be distilled to understand its value

What it isn't…

- DLP tools will not stop malicious behavior
  - They might stop specific malicious actions
- DLP is not a "Set it and forget it Ronco Showtime Rotisserie"
  - Requires constant time, upkeep and attention. Pretend it's a toddler.
- An end to your data security journey. It's just another data point to make you more nervous.

HOWMET AEROSPACE

Why you should run a DLP program

- Cyber security revolves around 5 key pillars (NIST CSF):
  - Identify – Figure out what you're protecting
  - Protect – Defend what you're protecting
  - Detect – Know when something goes wrong
  - Respond – Contain / stop the thing that went wrong
  - Recover – Restore and improve impaired processes

The NIST Cybersecurity Framework

- Understanding the details of **how** things went wrong, is arguably most important stage in this process. If you don't know that, you'll never improve.

- Without DLP, when the inevitable happens, you generally won't know:
  - What you lost
  - Who to tell
  - How your business will be impacted
  - The motives behind the attack

What makes for a successful program?

HOWMET AEROSPACE

How should this tool be run?

- Overheard at a Microsoft convention –
  - ***"… If the P stood for program rather than prevention, we'd all be in a better state"***

- During the RFP phase of our deployment, we spent significant time benchmarking with others and leveraging research / advisory firms to adopt best practices

- We were told one thing over, and over, and over again…

DLP is a **business** solution, not an IT one.

What makes for a successful program? (Cont.)

- So how does one create and operate a business run DLP program?

- Identify the goals of the program
  - Risk reduction, of course, but how?
    - Data visibility
    - Intellectual property protection
    - Personal information protection
    - User awareness

- Identify your stakeholders and their goals
  - Legal / Ethics and Compliance
  - HR
  - Privacy
  - IT (last for a reason)

- **Escalation procedure! (more on this later)**

Goals

- You **MUST** Prioritize your goals. Output from DLP is the definition of information overload

- Not all data is created equal.
  - You can't protect everything all the time – what do you want to focus on? How do you want to focus on that? Do you know where that data is? Is it classified? Is it somehow identifiable?

- Identify your company's risk appetite for escalations and intervention
  - When do you disable a process or system? When does HR / Legal want to be made aware of an incident?

- What level of control do you desire? Explicit blocking? Monitoring and logging only?

- How are you going to get users to conform to expectations? Published Policies? Best practices? Training?

Stakeholder responsibility

- Privacy (Data Protection Officer)
  - Reviews the tool **and** program to ensure consistency with company policies and localized regulations. This may vary from state to state, country to country.
- Legal
  - Support DPO's position and ensure that a Data Protection Agreement (DPA) is filed if needed
  - If Europe (and hence GDPR) is in scope, also consider a Privacy Impact Assessment (PIA) and DPIA (Data Protection Impact Assessment)
- HR
  - Likely key escalation point. Ensures company policies are current and consistent with how you expect high risk situations to be handled
- Ethics and Compliance
  - Validates your program operates within the company's values and expectations
- IT
  - Impact on environment (patches, network load, updates, reboots, etc.)

So something went wrong… Escalations!

You (Information security) should NOT be the primary investigator

What security knows

Technical data and evidence

- Detected an inconsistent / anomalous process
- Logs about what data was moved (where, when, etc.)
- Likelihood of this activity being conducted by an external threat actor

What security doesn't know…

Literally **everything** else

- **Business context** as to why that event was likely occurring
- The likelihood of this being malicious or due to a lack of education
- Employee status – are they in good standing? Have they put in their 2-week notice?
- Tactical engagement points within the business to better evaluate what happened

Summary of what makes a successful program

- **Prioritize** your company's goals and initiatives to determine what you want to focus on
- Enable yourself to be successful by being able to identify **prioritized data**
- Engage stakeholders **early** and get their input and views on how a program would be successful within **your** company
- Create metrics, communications, and incident reports that allow business leaders to co-run the program **with** you, instead of *supporting* you
- Create a **defined escalation plan** along with clear responsibilities. If IT has more than a 50% stake in this, it's almost certainly wrong.

Tool and vendor selection process

Tool and vendor selection process

- There are 3-6 key players in the DLP space, roughly the same for CASBs
- Each have their own strengths and weaknesses that need to be prioritized based off your company's goals.
- Some key factors that helped us make our vendor and product selections
  - Staffing
  - Culture
  - Privacy and Legal
  - Fit with other tools

Staffing

Question to guide your staffing level: How many incidents do you want to miss?

- You will never catch every incident, but more eyes results in more visibility
- DLP tools require dedicated FTEs. There's no avoiding it.
  - Splitting a resource here and there will be **ineffective**
- Smaller, midsize, and "cost conscious" companies commonly struggle getting value out of these solutions due to the heavy load on the organization
- Some DLP tools are meant to be deployed on-prem with moderate to substantial infrastructure deployed geographically dispersed. Others are meant to almost be exclusively cloud deployed.
  - Your ability to choose one over the other will likely come down to industry regulatory requirements as well as privacy/security decision points.
- Some DLP vendors sell DLP as a managed service or have partnered with service providers
  - Serves in a similar capacity to your MSSP but strictly related to DLP
- DLP is the definition of a solution that you get out what you put in
- **Key recommendation**: Start with "some". Let data and evidence rightsize your staff – leadership responds to data more readily than "maybes". **Strongly consider** managed services to augment your staff.

Culture / Privacy & Legal

- Culture / Privacy & Legal all go hand in hand due to the nature of the tool

- When making decisions, consider what is possible versus configured on your tenant
  - Unions, works councils, and others will likely search for data on the product and could assume that's what you will be doing, regardless of your configuration
  - Some solutions can be significantly more invasive than others, some even record screens when certain actions take place

- Some tools focus on metadata collection whereas others also capture and store content.
  - Are you intentionally avoiding seeing actual user data? Do you need it due to regulators?

- **Key recommendation**: Select the **least invasive** product based on your goals and visibility desires. More data does not simply result in a better program.

Fit with other tools

- We all battle the YAA challenge - Yet Another Agent!

- Many DLP tools have similar capabilities but differ in the way the data is presented.
  - Many have one “niche” capability that the others are missing. Make sure you understand limitations of the products and don’t accept that your use case is covered because a competitor could easily do it.

- While evaluating tools, consider the totality of your endpoint solutions and whether you have duplicated services.
  - Many DLP vendors are making their tool a full Endpoint Detection and Response (EDR) solution
  - It’s likely that there are cost takeout opportunities, especially if you’ve hit a “good enough” level of capability for your goals

- Many of these tools are embedded within the kernel – make sure there are no incompatibilities with each other (like two anti-malware services running simultaneously)

- **Key recommendation**: Heatmap your endpoint capabilities and review what you really need. You may want to pay more for a more advanced product to take something else out or get a cheaper one to supplement gaps in an existing robust endpoint solution set.

What you may find...

Disclaimer

- **The discussed categories of incidents are the high-level types of incidents that can occur**
- **They come from industry stories, best practices, and personal experience**
- **They have not necessarily occurred at Howmet Aerospace**

What you may find

DLP incidents generally fit into one of three categories

Intellectual property misappropriation

- Data being intentionally or accidentally mishandled (internal or external threat)

Personal Identifiable information data incident or data breach

- Personal data of employees, customers, or other third parties entrusted to you as a data controller

High risk business transactions

- Technical definition: "The things that make you stop and want to go home for the day"
- Regulatory, policy, or common-sense violation

Intellectual Property Misappropriation

- Generally, IP misappropriation is taking or using intellectual property that does not belong to you
- Internal vs external threats, as well as accidental vs intentional mishandling all have different escalation paths and disclosure requirements
- Criminal charges can be challenging to pursue when the offence is caught proactively (before there is realized financial harm to the company)
  - Imagine calling the police in a busy city because someone tried to take a piece of jewelry through a window but dropped it and then ran…

- **Key Recommendations**:
  - Ensure company policies and expectations of your users are explicitly clear in terms of what is and what is not permitted regarding data handing
  - Ensure there is education on what intellectual property is and who it belongs to (*Hint, it's almost **never** the user*)
  - These tools generate a LOT of data. Use that to make risk-based decisions on what processes and services you will continue to allow, and how. (coach vs block vs encrypt)

Personally identifiable information risk

- Understand and use correct terminology when it comes to PII risk
  - PII **incidents** are caused by unauthorized use or disclosure of information
  - PII **breaches** are incidents that have passed regulatory minimums (often based on likelihood of risk) that define them as breaches.
  - It is often up to you to self-declare a breach vs incident.
  - The difference between the two is important and largely defines your post-incident actions as well as reporting requirements
- Process, service, and data field mapping can help inventory where your risk points are
  - Anyone who has done GDPR is likely familiar with this
- Localities are implementing their own privacy laws, complicating disclosure.
  - Your company is based in NYC, the European citizen subject lives in California, the breach occurred in your Virginia data center.

- **Key recommendations**: Prepare breach processes **ahead of time**. Many regulations have FAST disclosure requirements. Align with your Legal teams on what breaches vs incidents are, and ensure you are weighing the interests of data subject and the company.

I was sleeping and just woke up… what should I know?

- DLP is a business process that demands active participation from business stakeholders
  - Do **NOT** run it has an IT solution
- Optimize your tools to your program goals, **not** flashy capabilities
- Classify / prioritize your data in some meaningful way
- Be mindful of "totalitarian" enforcement thinking that will solve things
  - Imagine you plug one hole on a boat that has 6 others - what happens?
- Know that you will find things. Prepare **now** for when the inevitable happens.
- When responding, **determine early** whether this is an internally or externally caused event
- Ensure that company policies match data handling expectations
- **EDUCATE EDUCATE EDUCATE**
  - Users are incredibly resourceful and creative. They will find any possible way to do their job as efficiently as possible.
  - If users don't seem to "get it" – you've failed. Not them.

Questions?


HOWMET
AEROSPACE