Rethinking Vulnerability Management

Shifting ownership from IT to the business

When it comes to vulnerability management programs, not much has changed over the years. We see programs using the same, or similar, technologies to detect and identify vulnerabilities within their infrastructures and applications. Resourcing and staffing has not really evolved, even with the face of vulnerabilities growing into insurmountable numbers. Reporting and metric's (KPIs or KRIs) are getting a lot of attention but continue to miss the mark on being successful with executives or the board of directors. Breaches continue to own headlines and as a result companies are facing more pressure to remove vulnerability risks and secure their business.

A different approach

At Iceberg, we believe that to drive better business results from vulnerability management programs, companies need to revisit how they approach the data within those programs, and what needs to change to get better results. Traditional programs begin and end mostly within IT, from the time of discovery, through analysis, remediation and then reporting. Programs typically start with a vulnerability that has been discovered on an IT asset, and then analysts try to figure out if the vulnerability risk should increase or decrease based on what the asset means to the company.

But what if we looked at it differently? What if our vulnerability management program started with what business processes and services are important to the company, and worked its way back to the vulnerability?

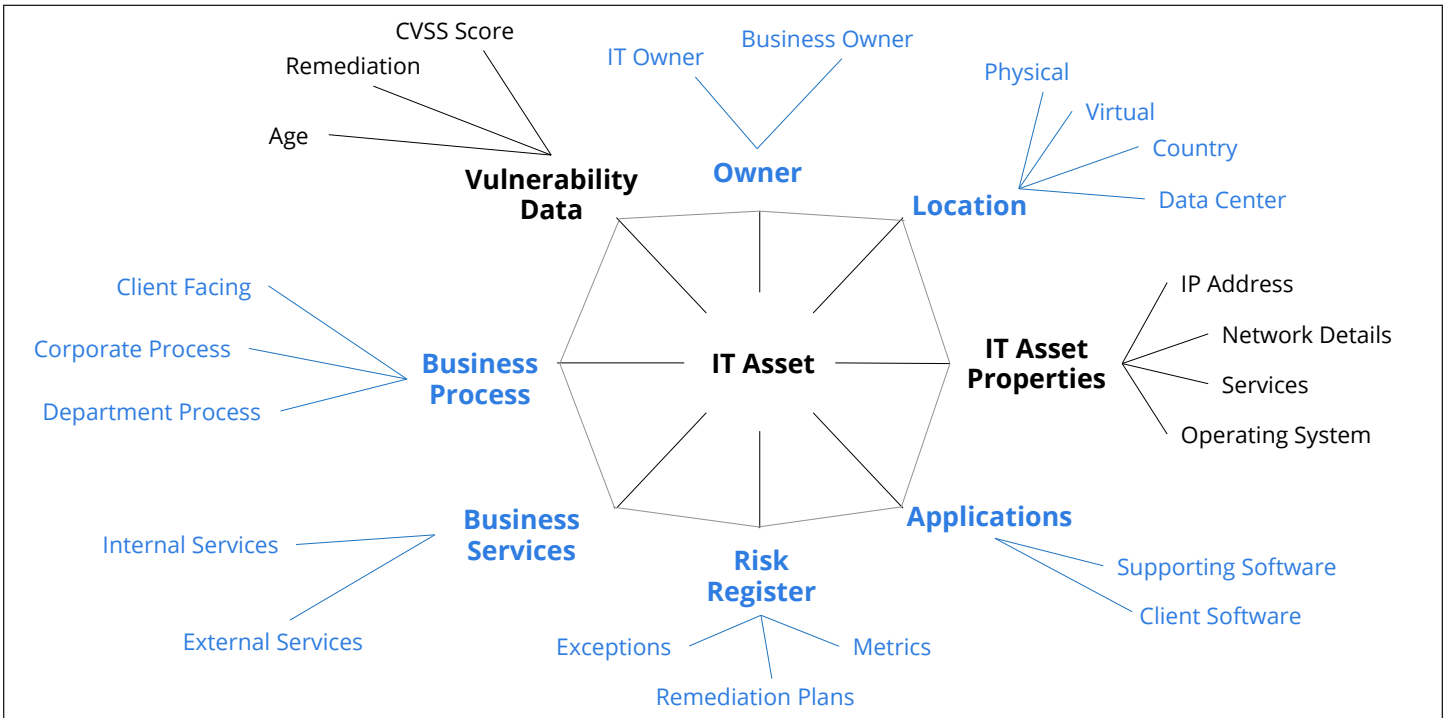
What if our vulnerability management program started with what business processes and services are important to the company, and worked its way back to the vulnerability?

We need to redefine how IT departments analyze vulnerability and who should be accountable for the risks that come with vulnerabilities. Vulnerability management programs are in place to protect the product and services that companies offer. IT will always own the asset, but the business will always own the asset's purpose. Therefore successful programs need collaboration with both IT and the business to share accountability for vulnerability management and the risk they impose on the business.

How should vulnerabilities be prioritized?

Typically, when vulnerabilities are identified, they are given a rating (or score) provided by a scanning vendor (originating from the technology vendor or industry). That rating gets passed to the asset and in some situations, that same rating is applied to the business products or services that the asset supports. The question becomes, should these vulnerability ratings be passed to the business function to identify risk? Or should the business function influence the vulnerability rating driving a business risk? A strategic change of approach is needed to drive better results in vulnerability management and the business function should influence the vulnerability ratings, and therefore drive the overall business function vulnerability risk rating.

By David White
Senior GRC Consultant, Iceberg
dwhite@icebergnetworks.com



Adding Business Context: *Traditional vulnerability management programs are focused on IT-centric factors, shown in black on this diagram. A business-centric approach adds additional context, shown in blue.*

Where do we start?

At this point you may be thinking, *"Great, we have vulnerability data from our scanners, but we don't have a good inventory of our business products and services and the assets that support them. Is this a show stopper for me?"*

In order to mature your vulnerability risk management program, missing data cannot be a show stopper or the maturity of the program will fail. Iceberg has developed a proven methodology for conducting workshops to collect, analyze and structure business products and services data elements to be used in calculating vulnerability risk ratings. Defining business products and services is critical to the success of maturing your vulnerability risk management program, and therefore it goes without saying, establishing a sustainable process to maintain the data integrity of the products and services is equally important.

Although business products and services are critical data elements, building additional context layers allows for more granular and accurate risk calculations to be performed. Understanding the business hierarchy and business processes that are related to product and services allows for more granular reporting. At the same time, understanding the people and locations associated with business functions and IT assets, could provide alternate paths for remediation activities and also influence the risk. Remember, we are not just calling out how many vulnerabilities we have, we are identifying which business products have vulnerabilities, and defining when they are expected to be fixed.

We need to redefine how IT departments analyze vulnerabilities and who should be accountable for the risks that come with vulnerabilities.

The value of a GRC platform

At a fairly high level, I have described a non-traditional way to look at vulnerability management. Instead of looking at it from the asset view, look at it from the business function view. As alluded to earlier, this is easier said than done. What about all this new business context data collected that now needs to be managed with a sustainable process?

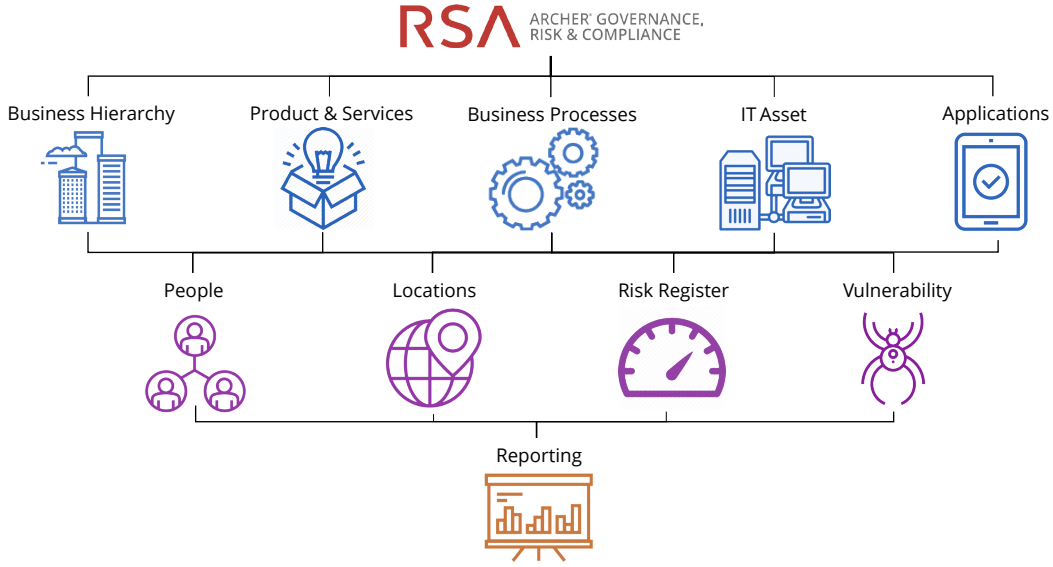
This is where a Governance, Risk and Compliance (GRC) platform becomes the backbone for building all the context required for a more effective vulnerability management program. At Iceberg, we work very closely with the RSA Archer product to manage both IT and business content, enabling context-aware vulnerability risk management programs. With RSA Archer's Threat Management platform, Iceberg helps clients build programs to identify and manage risk to the business.

With RSA Archer, Iceberg helps companies build programs that measure risk to the business in a single pane of glass. Aggregating IT and business data into unified calculations allows vulnerability management programs to truly represent the dynamically changing risk scores to the business that result from the constantly changing state of asset vulnerabilities. This process ultimately facilitates a program for reporting and metrics that will serve both operational activities as well as executive briefings.

Value and impact

Organizations who take this collaborative approach, and shift ownership and accountability of vulnerabilities to the business side, will typically see a significant overall reduction in the number of open vulnerabilities, and acceleration in the timelines for remediation of identified issues.

As mentioned earlier, vulnerability management programs are in place to protect our businesses products and services. As we continue to build and mature these programs, organizations need to start bringing the business into the equation to help build more meaningful reports, better metrics and more efficient remediation plans.



With RSA Archer's Threat Management platform, Iceberg helps clients build programs to identify and manage risk to the business, incorporating IT and business content to enable a context-aware vulnerability management program.

Iceberg
Delivering Risk Intelligence

Iceberg Networks (US) Corporation
67 Bedford St., Suite 400 West, Burlington, MA 01803
Toll Free: 855-595-0808 • info@icebergnetworks.com
Twitter: *@icebergnetworks* • Blog: *icebergnetworks.com/blog*

RSA SECURWORLD STRATEGIC PARTNER