I’ll be honest, I’m not waiting with bated breath for the next Forrester or Gartner study on data risk and cybersecurity. I don’t always find the report suggestions practical for organizations like ours. But sometimes, we see data that makes us stop and think about how we’re actually responding to the changing nature of data risk. And that’s just what happened when a prominent industry analyst firm highlighted at an event this winter that 80% of CEOs are changing their company’s culture to accelerate their digital business strategy – ultimately, to grow. Combine that with a global health crisis that propelled us within a matter of days into a remote work reality, which we had previously anticipated happening gradually over the next five years, and we find ourselves in a world where the priority of making employees productive is accelerating data security risks faster than we can even assess.

As institutions empower faculty and staff with new collaboration technology — from Gmail and Slack, to project management tools and code repository apps — the places where research data lives and moves are fundamentally changing.

And here’s the deal: security teams can’t address these risks alone. In my position helping a variety of organizations build effective security processes and programs, I have seen a few security teams quickly address data security vulnerabilities by simply engaging institution partners — and not with the traditional security awareness programs. HR teams, legal and line of institution leaders can play a critical role in data security in this era of collaboration and working from whatever location you’re productive.

We’ll summarize here the four common, yet critical, attributes of successful security organizations, regardless of their maturity:

1. They help their stakeholders understand the situation

Today, the emphasis on productivity is essential, but so is addressing the risk that new tech and working patterns introduce. What do stakeholders need to know right now?
Many traditional security tools rely on faculty & staff being connected to the campus network. Increasingly, they are working off-network – so security misses a lot of visibility into how data moves. Tools that deliver endpoint visibility via an agent or without requiring data to flow through a VPN are suddenly in-demand.

Also, when people are working from home, they tend to feel more comfortable and work as if they were using personal devices. Basic security hygiene should not lapse when faculty and staff work off campus.

Exfiltration or misuse of institution data doesn’t have to be malicious. In fact, it isn’t in most cases. Simple mistakes happen. And people use tools that help them get their jobs done efficiently. In fact, more than a third (37%) of employees told Code42 recently that they use unsanctioned apps every day to share data with their colleagues. It isn’t that security teams don’t trust faculty and staff or want to police the institution. Instead, they want to understand where vulnerabilities are so they can adapt existing protocols and ensure the right tools are in place to productivity.

Security teams know that collaboration tools aren’t going anywhere and that they’re essential for the modern institutions, so security is adapting and needs the help of internal partners.

2. They get key stakeholders to understand the implications and urgency of data loss — by being transparent and realistic, but not sensational.

Ok, we know the response you’ll get to the last bullet above is “You need my help? Take a number.” Up the priority by highlighting what data loss means for them (but don’t be over the top).

Frame the situation in a useful way for your audience:

- Senior researcher? Talk about the possibility of losing research data, sabotage, or negligent sharing. Losing the confidentiality of that data means you won’t be first to publish with your findings and could lose future funding.
- Head of legal? It’s not all about compliance. What security is trying to do is get ahead of the inevitable investigation and protect data from loss or misuse early, so that costly litigation is less necessary helping to prevent reputational damage.
- Head of compliance? Help assess extent of a data breach in order to limit the cost of potential fines.
- Head of HR? Look, security’s not the morality police, and this new world isn’t changing that. So, be clear that security wants to follow the data, not the people. Make a plan early to get HR the data security info they need to protect the integrity of your company’s culture without requiring that security teams invasively surveil users, or that HR teams become experts using complicated security tools to pair data activity to users.
  - Quick win: here’s an eBook you can send your HR leader on the security costs of employee turnover.

3. They make a plan early to address data security at scale during periods of change.

Faculty and staff are still going to resign. People are going to act carelessly with data. Institutions are going to restructure. Get your stakeholders involved in making a plan and be sure not to let the intimidation of a big program get in the way.

- Start with quick wins, not a full-blown program. Plan for data security and visibility into where data lives and moves during off-boarding; ask about and see the riskiest behaviors with shadow IT and mirror technology, and prepare for endpoint visibility in remote work.
- Look for context — ask your institution partners what’s normal and strange. Without context, tracking data is all just file events. Is it normal for researchers to use file-sharing tools dictated by outside collaborators or for visiting faculty to leverage their home institutions’ collaboration tool? Which staff members should or should not have access to recruitment or donor reports from Salesforce?
- Code42 helps institutions address data security using tools like ours to improve the speed and accuracy of insider threat detection, investigation and response. Code42 delivers the risk signal needed to distinguish between everyday collaboration and the events that actually put institutional data at risk.
4. Be transparent with your leadership team. It encourages better behavior.
   • You don’t have to share the details or the keys to the kingdom, but remind people of acceptable use protocols and let them know that you’re monitoring data use.
   • The response to insider threats to data isn’t the same as a traditional IR or SOC response. And in most cases of mishandling data, the response won’t require punitive action. While you’ll certainly want to be prepared for how you and your institution partners will handle malicious theft of data, the most common response will be some education and security awareness – not only with faculty and staff, but with leaders to help them understand the inadvertent risk an institution can incur when teams misuse or exfiltrate data.
   • It’s easier to be transparent when you’re monitoring data use instead of faculty and staff themselves.

Institutions are rapidly responding to their environments and pushing for digital-first strategies. It’s time to embrace the collaboration culture by empowering security organizations to create a strategy that enables that culture.