Member's Quarterly Summer 2019 Edition

Feature

Investigating an Employee's Digital Activity

What HR needs to know

Brian Sartorelli
President, CEO, IRM (Investigative Research Management)

Ryan Duquette
Founder/Principal HEXIGENT Consulting

You've been asked to review the digital activity of an employee. Your employer has some concerns and wants you to investigate. With the amount of enterprise-level technology and controls that most companies now have, shouldn't that be fairly straightforward? Not always. While the tools and methods used to perform digital investigations are usually well defined, there are some 'grey areas' around what you should and should not be looking at and why that matters.

Here are our top 5 things to consider before starting any internal investigation into an employee's digital activity.

1. Ensure you have authority to proceed

While the employer might suspect some kind of foul play such as intellectual property theft and asks you to investigate an employee's digital footprints, it's important that you understand what's permissible before you do anything. Just because the staff member was using a company asset, this does not always translate to an open opportunity to review everything they've been doing.

Before you begin, get a formal request from the organization in writing. This should define the scope and give you appropriate authority. Make sure it has the appropriate sign-off from management and keep all communication relative to the request and the investigation itself. It may be beneficial to have your legal department or counsel involved or at least informed from the start, as the matter could end up in court or a tribunal and you'll need to prove everything you did and why.

2. Check corporate policies

Review your company policies to determine what an employee is allowed to do (and more importantly, not do). Establish if there is content which relates to activity monitoring or reviews. Where possible, confirm that employees, and specifically any which are in scope for your investigation, are aware of these policies. The security department of your organization may have a list of those who has gone through awareness training, while your HR department would typically have a list of staff who have signed off on policy compliance. Ideally, you need to confirm that the employee has read the policies, had awareness training and signed off on their understanding.

If no policies actually exist or there is no requirement for employees to read them, then it can be argued that they were allowed to do anything with the corporate systems since no restrictions have been imposed.

3. Determine compliance requirements

Depending on what business your company is in, you may find that they're obligated to comply with a standard or framework that may either a) limit your ability to directly review activity, or b) put your company's compliance status at risk should you proceed. A number of these frameworks are security focused,

Member's Quarterly Summer 2019 Edition

Feature continued

so a discussion with your information security teams may provide some useful insights. If your company has a risk and/or compliance function (or similar), they may be able to highlight any areas of concern.

Check to make sure that what you're looking to do is achievable. Also, check to see if the role of the employee may require them to have privileged access to highly confidential data (such as payment card numbers, personally identifiable information or financial data) and that your review does not compromise the organization's good standing.

If your company holds federally classified data, find out exactly to what the employee had authorized access. If it's above your own clearance level, you may need to call in someone with appropriate clearance to handle the data. While you may not be looking to review any of the data itself, just you having a copy of it or access to the system that holds it may cause an issue.

4. Focus the scope of the investigation

Many times we're asked to find 'anything of relevance'. That should never be readily agreed to without first knowing the facts. Let's say that a staff member is leaving the company and it's believed they had stolen confidential intellectual property. Using digital forensic methods and tools, it can often be determined what they did and how they did it. Network and system logs will show general activity. An in-depth forensic review of the systems and devices that the employee used could provide a very granular view of what they did. While this is great news for most investigations, there can be some challenges. If you were to start looking at everything that was done, your review could take weeks or months. It could also take you down a path that has nothing at all to do with the original request.

The investigation should be focused. There should be rationale for what you're doing and the evidence you are looking for should be well defined. Using the above example of intellectual property theft, you ideally want a listing of what data the employee is suspected of removing, during what time period, if the data is vast and just considered a 'type' (such as "spreadsheets"), what common terms, phrases or language could it contain. Knowing all of this will speed up the investigation, help your legal counsel be comfortable in knowing that you weren't going on a 'witch hunt' (which can be a common argument by the defense in legal proceedings). This will let you get to the relevant facts more efficiently. If you receive an investigation request and you're uncomfortable or feel that the scope is too broad, you should collaborate with your management to gently educate them as to why a defined scope is needed.

That being said, with many fraud and other investigations, evidence can point to areas that may be beyond your original scope. In situations such as these, it is important to communicate your findings and return to step 1.

5. Check privacy laws and legislations

Depending on your location, you may have to consider various privacy laws and legislations before starting any employee investigation. Legislation is usually relevant to the location in which the work is being performed. For example, if you're being asked to review user activity for someone operating from a regional office in Germany, the fact you are based at head office in Toronto does not mean that Canadian privacy law will necessarily apply. In that example, the German Bundesdatenschutzgesetz (BDSG) has very strict guidelines as to what can and can't be done with employee data contained on work systems (including the transferring of any data outside of national borders). It's always best to check with your legal counsel and compliance department before conducting any investigation on employee data. Not doing so may jeopardize the validity of your findings.

Member's Quarterly Summer 2019 Edition

Feature continued

There may be other factors to consider depending on your organization and the type of investigation that you are conducting. Always remember that any investigation that you conduct on an employee may result in legal action and potentially litigation. You may have to testify in court as to the actions that you took so it is imperative that you document everything you do and communicate your actions with other stakeholders involved.

Once you have considered all of the above and you're reasonably sure of compliance, then we suggest that you contact a digital forensic company for the investigation. In situations such as this, retaining a third party is highly recommended.

Brian Sartorelli is President/CEO of IRM (Investigative Research Management) and can be reached by email at brians@irmi.ca.

Ryan Duquette is Founder/Principal at HEXIGENT Consulting and can be reached at ryanduquette@hexigent.com.