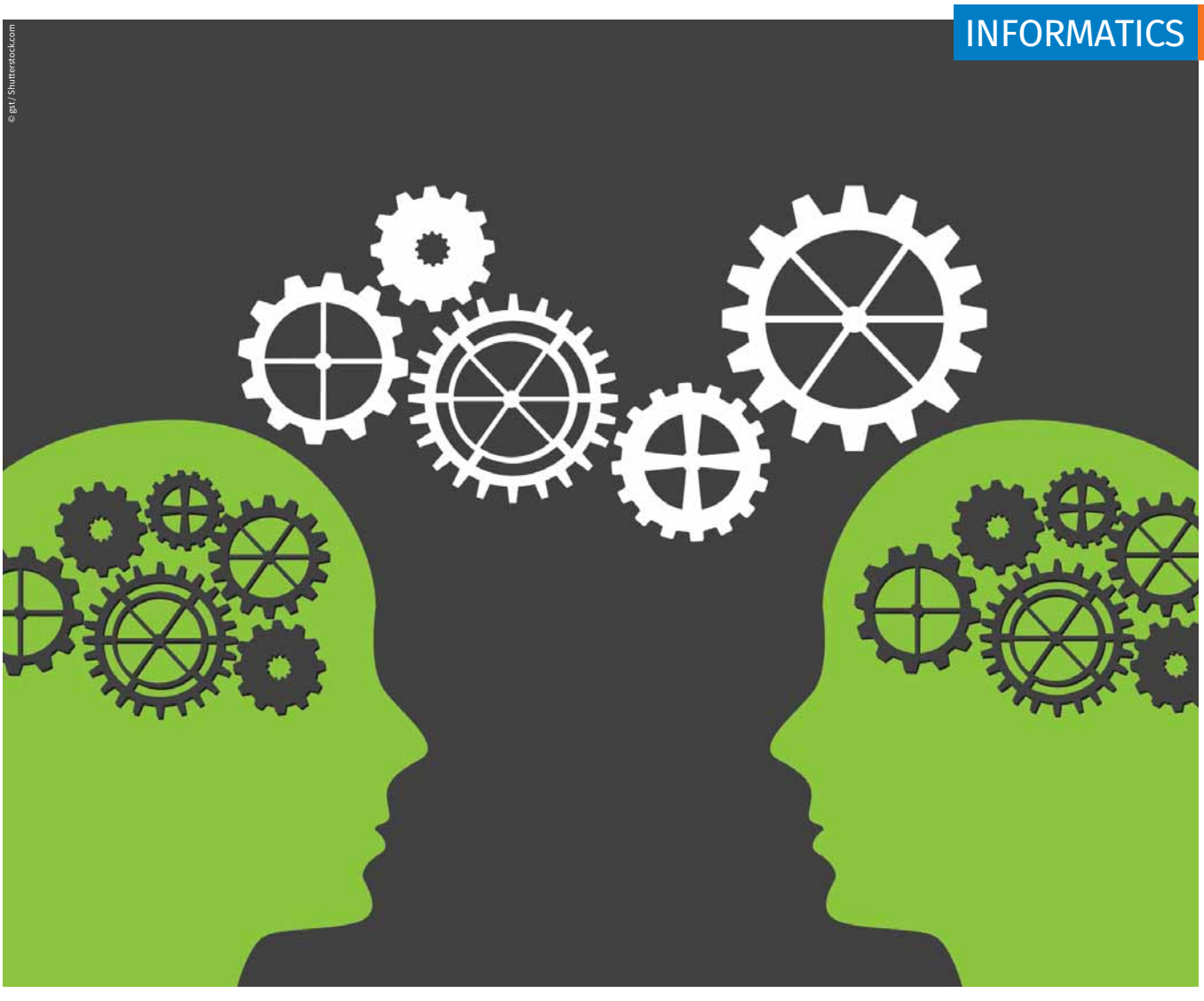


# Security considerations for external research

**Michael H. Elliott**
Atrium Research & Consulting

**Intellectual Property (IP) is the lifeblood of the pharmaceutical industry. Without it, there would not be much of a business. Growing research and development globalisation, externalisation, the expansion of electronic data management systems and the lack of consistent global IP enforcement is increasing the capacity of external and internal parties to steal trade secrets. A risk-based framework is therefore necessary to identify and remediate areas of vulnerability.**

## Increasing dangers of IP theft

The possibilities of IP theft have never been greater. Losses cost businesses as much as $300 billion a year in the United States alone. Life science organisations are particularly at risk given the high value of the IP and the levels of research and development investment. According to a study conducted by Kroll in 2015, 13% of healthcare, pharmaceutical and biotechnology companies experienced IP theft in 2014; higher than any other industry studied. 80% of life science respondents indicated that their exposure to fraud has increased, due primarily to high staff turnovers and an increase in out-sourcing. Astonishingly, only 18% of companies planned to enhance protection in 2016, despite the millions (or billions) of dollars of potential negative impact.

When you ask IT professionals or business leaders where the biggest threat of IP loss originates, most point to hackers gaining remote access to systems. This has been cited as one of the major

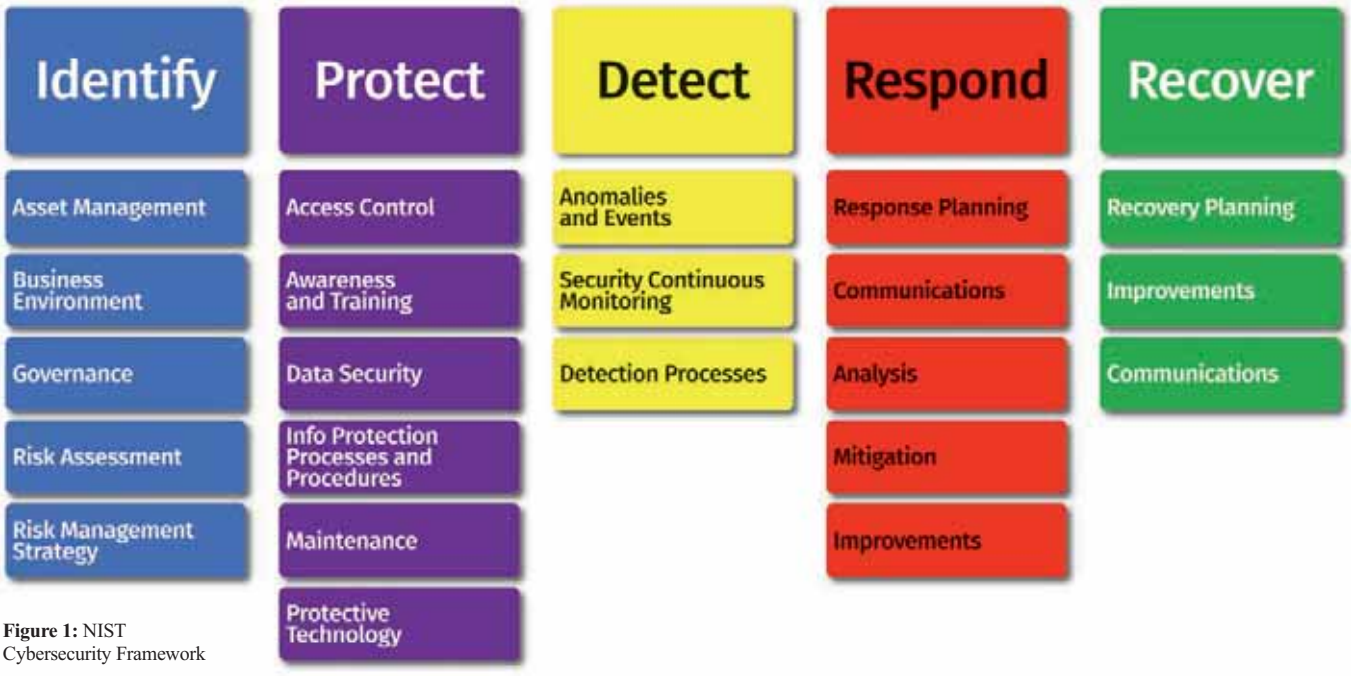


**Figure 1:** NIST Cybersecurity Framework

reasons why the industry has been so reluctant to adopt cloud technology for drug discovery. The fear has been that if IP were maintained in the cloud, then a cybercriminal would somehow have easier access to trade secrets.

However, in their study, *Privileged User Abuse and the Insider Threat*, the Ponemon Institute said, "In reality, the big risk is on the inside as opposed to externally. 44% of organisations view the prevention of insider fraud as a top security priority." Verizon indicated that 46% of threats to IP are from internal breaches; the greatest single source. However, insiders are not always alone. "For outsiders wishing to get at it with minimal risk and effort, recruiting insiders to participate often makes a good deal of sense," according to the Verizon report. Making matters worse, Symantec asserted: "Half of employees admit to taking corporate data when they leave a job, and 40% say they plan to use the data in their new job." The same study goes on to say that "56% don't think it's a crime to use trade secrets taken from a previous employer." Even more frightening are the results from the recent Sailpoint Market Pulse Survey: one in seven employees would sell their password to a third party for as little as $150.

> "When you ask IT professionals or business leaders where the biggest threat of IP loss originates, most point to hackers"

Risks are not theoretical; they are real. Here are a few examples:

- Earlier this year two scientists at GlaxoSmithKline were indicted in the US on charges of stealing oncology research data. They allegedly emailed and transferred data to associates who planned to market the information through a company they created in China.
- An engineer for Becton, Dickinson and Company stole data on a disposable pen injector under development. The engineer downloaded over 8,000 files to external storage devices in the hopes of taking the data back to India to start a new company.
- A former Sanofi-Aventis chemist pleaded guilty to stealing trade secrets and attempting to sell them through a Chinese company. The scientist accessed internal Sanofi systems and downloaded chemical structures to a thumb drive.
- A Boston Scientific engineer pleaded guilty to downloading secret plans for a new medical device to a flash drive. He was attempting to take them to Vietnam to manufacture his own version of the device.

The aforementioned scenarios were detected by diligent reviews of system logs and technology such as digital loss prevention. Yet these are exceptions, as few companies – especially smaller ones – have procedures and the technology to monitor the user activity of systems such as registration, laboratory information management system (LIMS), electronic laboratory notebook (ELN) and document management. It does not matter whether the data is in the cloud or on premises. Theft may just come from someone who is actually authorised to use the platforms you already have.

Upon visiting a top fifteen pharmaceutical company a few years ago, a scientist very clearly made this point when he showed me a flash drive he had in his possession. "I downloaded our entire registration database," he said. "No one even noticed." He was not doing anything malicious, just making the point that the company rarely tracks downloads and data usage. So, how many malicious activities are happening that are not even detected? Quite a lot, it seems. According to the Verizon report, "All too often, evidence of events leading to breaches was available to the victim but was neither noticed nor acted upon."

## Enter the world of externalisation

It is bad enough when you have to worry about the threats from cybercriminals and internal users. Externalisation now constitutes close to 50% of total R&D spending and is growing, particularly in discovery. In this segment of patentable ideas, research virtualisation is growing

by more than 20% a year. It is not uncommon for a major pharmaceutical organisation to have in excess of 100 partners, ranging from consortia on target identification to bioassay contractors to clinical study managers. On the other end of the spectrum, an estimated one third of venture funding now goes to virtual biotechs who outsource all scientific activity.

In many cases the external party is treated as an extension of internal resources. Instead of hiring ten chemists in the US or Europe, a company could gain thirty or forty equivalents from a contractor in China. These are resources the company may never meet, let alone be in a position to vet their backgrounds. This makes economic sense, but given both their location and treatment as internal resources, risks are increased. It is not to say there will be an incident. There may never be. But, given the parameters of the relationship, those risks should be evaluated.


***In vitro* screening data are among the data types that require systems to manage**

Bridging the data flow between parties in a partner network can be quite complex, especially when the collaboration is more than a simple point-to-point transfer. In a complex network like a consortium, there are many different data types, formats and systems used by the various participants. Companies often consider whether they should just expose their internal systems as teams could freely collaborate and have real-time data access. They are then faced with the on-going administrative burden of on-boarding and off-boarding users and managing user rights.

> “All too often, evidence of events leading to breaches was available to the victim but was neither noticed nor acted upon”

The movement of data and material between parties makes it unlikely that a single technology platform could serve all capabilities except within a specific domain (e.g., toxicology or medicinal chemistry). Systems are necessary to manage material logistics, task workflow, *in vitro* screening data, *in vivo* study data, stability, clinical data capture and so forth. The administrative overhead and the dissimilar security capabilities of each platform increase complexity. Do you really want to expose your ageing registration platform that does not have row-level security to an offshore contract employee just because it is easy to do so? It is no wonder that over 75% of data shared between partners in discovery research and preclinical development is in the form of a document sent via email or shared through systems such as SharePoint. That is inefficient, both operationally and scientifically.

| Partner | Type of Partnership | Risk | Data Flow | Data | Systems |
|---|---|---|---|---|---|
| Large Pharma Collaborator | Full strategic partnership, co-development | | Bi-directional sharing of programme data | Large number of file types. Agreement on formats | Share multiple technologies. Isolate from other internal. Project/role-based security |
| Small Biotech | In-licensing at new molecular entity (NME) | | Bi-directional sharing of specific project data | Isolate project and partner specific data | Isolated platforms for collaboration |
| Large University | Target id and validation | | Minimal data to partner, one-way transfer of data | Isolate data, blind targets, encrypt sequences | Extract, transform and load (ETL) into existing platforms |
| Preclinical services CRO | GLP toxicology services | | Compound out, report back | Blind compound and internal IDs | Use of partner systems. Post to validated collaboration space |
| Large Offshore CRO | Low-cost *in vitro* screening services | | Compound out, structured data back | Obfuscate all structures, double blinding (targets, compound id, etc) | Encrypted teansfer from contactor, ETL bioassay data to warehouse |
| Synthesis House | Low-cost chemical library synthesis | | Transfer structures and analytical data at end of experiments | No transfer of metadata, only library design. Verify structures | Isolated, cloud ELN and SDMS |

**Figure 2:** Example of a plan being created based on the type of partnership

## Analysis of risk

There are many frameworks for securing critical assets to improve an organisation's cyber defense maturity. These include: ISO 27002, HITRUST, COBIT, COSCO and the NIST Cybersecurity Framework. Shown in **Figure 1** (page 18), the NIST framework transitions from organisational understanding to the implementation of safeguards through recovery from events. These frameworks are used to build a comprehensive strategy for the entire environment, including the protection of IP and trade secrets.

Each of the frameworks mentioned share a common element of risk assessment. The appraisal includes identifying what the risks are; how to quantify them; and the level of risks to be assumed. As risks are interrelated, analysis must be viewed holistically, instead of evaluating individual systems or workflows. Consider, as an example, that PharmCo has two contractors: medicinal chemistry contractor A knows the structures and screening contractor B does not know them. B is performing *in vitro* and *in vivo* screening. Both are in the same city and have a high turnover of employees. Unfortunately, both have been given un-blinded compound identifiers. This allows a scientist moving from A to B to understand the activity of PharmCo's structures, taking the most potent of them to a company he is starting.

Within a partner framework, one must evaluate 'risk exposure', which is the likelihood of an event occurring multiplied by the consequence of the event. In our consulting practice, we associate the inverse of likelihood to a 'trust' level. The higher the trust level, the less likely events will occur. Some questions to evaluate trust include:

- How long have you been working with the contractor without incident?
- What is the history of services?
- How well do we know the users? Are there background checks on the employees?
- What is the nature of the contractual agreements?
- What risks did our vendor audit expose?
- Which country are they working in?

Consequences can range from catastrophic (taking the entire registration system) to insignificant (single assay for a blinded drug product). They are dependent on the type of data and information shared with the partner organisation.

Every organisation has a bespoke evaluation system based on a situation analysis and the risks they are willing to assume. What might be considered high risk for one may be low risk for another. An upstart virtual company with ten employees has a different profile to a top ten pharmaceutical firm with thousands of employees and billions of dollars in revenue. In any case, valuation can be assigned to trust levels and consequences to determine areas of greatest threat. The risk exposure is measured against the controls in place to highlight gaps requiring remediation.


**There are several industry-standard frameworks that enable companies to protect IP and trade secrets**

> "The externalisation security strategy must be tuned to the nuances of the different partner relationships"

A plan is then developed based on the partnership, risk level and types of data exchanged. In the example shown in **Figure 2** (page 19), the risk exposures conclude distinctive levels of control. For a low-cost synthesis operation, an isolated cloud ELN is used to completely segregate internal systems. Obfuscation is used on project IDs, targets, compounds, etc. For a joint-venture partner where there is shared risk, common systems are used, but are isolated from other systems in the environment.

Risk analysis is just the beginning of a comprehensive cybersecurity strategy. Following the NIST framework, there must be an organisational commitment to governance, protection, detection, response and recovery. Organisations must give particular attention to detection; any systems can be breached, so it is essential to detect events and know how to respond.

The expansion of research virtualisation is increasing the danger of IP theft across many dimensions; cybercriminals, malware, country-sponsored theft, contractors and even internal employees. The greatest risk is a lack of security awareness and unwillingness to treat it with the utmost urgency. Best practice organisations utilise a framework for risk management and cybersecurity. They develop strategies, train users, audit contractors and continually test and monitor platforms. That being said, it is impractical to utilise a one-size-fits-all methodology across all partners and contractors if research is to progress. The externalisation security strategy must be tuned to the nuances of the different partner relationships, their trust levels and the types of data shared.

**Michael H. Elliott** is the CEO of Atrium Research & Consulting, a company he founded in 2003 to provide scientific informatics market research and strategic planning services. His career began as a bioanalytical researcher where he developed mainframe software for data analysis. In 1983, he joined Perkin-Elmer Corporation, as a LIMS technical specialist. His career at PE progressed from LIMS sales to VP and GM of the pharmaceutical analysis division. In 2000, he joined Scientific Software, Inc. (now part of Agilent) as SVP responsible for product management, marketing, sales, support and customer service. Mr Elliott has authored multiple research studies on laboratory informatics, has over 30 published articles and has presented in over 25 countries.