Pretexting Prevention: Minimizing Inbound and Outbound Risks

An Axentis White Paper
Matthew Leonard—CIPP and Senior Fellow of the Ponemon Institute
Ted Frank—President and Co-founder Axentis, Inc
Pretexiting Prevention: Minimizing Inbound and Outbound Risks
An Axentis White Paper

Pretexiting: The Two-Fold Risk

Pretexiting – the acquisition of confidential information by fraudulent representation of one’s identity – has received a lot of attention recently because of its role in the HP board scandal. But pretexting has always been with us. It has been called “social engineering” when referring to a hacker tricking a computer user into revealing a password. It has also been considered by some to be simply a “sharp” or “aggressive” business practice – as in the case of a salesperson getting the inside scoop on a competitor’s plans or even just getting past a secretary. By any name, however, pretexting poses a significant threat to business of all kinds.

The risks associated with pretexting fall into two basic categories:

1) Inbound risk
Companies that fail to fully safeguard themselves against the pretexting tactics of others can compromise confidential data (including that entrusted to them by their customers), expose intellectual property, and prematurely reveal their plans to the outside world. By allowing themselves to fall prey to pretexting, these companies can lose the confidence of the market, suffer financial losses, and open themselves up to legal and regulatory exposure.

2) Outbound risk
Companies that fail to effectively prevent the use of pretexting tactics by their employees and contractors can find themselves in the same situation as HP. The careers of top executives can be ruined. Brand identity and reputation can be eroded. Regulators can impose substantial fines. It is even possible that someone will have to spend some time in jail.

It’s important to emphasize both of these types of risks extend beyond the actual boundaries of the enterprise. Suppliers, outsourcers and other business partners can also create significant exposure to both types of risk. On one hand, they may be provided with confidential information that, if inadequate safeguards are in place, they may surrender as a result of pretexting. On the other hand, as occurred in the HP case, they may themselves engage in pretexting in order to fulfill some assigned objective. In either case, culpability can be assigned to a company or individuals at that company even if the pretexting itself was performed by someone outside the company.

So how can companies best protect themselves from both inbound and outbound pretexting? How can they best minimize the impact of pretexting incidents should they in fact occur? And how can they know whether they’ve actually been effective at minimizing the likelihood and the impact these two types of pretexting risks?
The Five Core Elements of
Pretexting Prevention

It would be nice if there were a simple
technological solution to the pretexting
problem. But there isn’t. You can’t install a
computer chip in the brain of every
employee and contractor that can alert you
when they’re about to be duped by an
attempt at pretexting or are planning such an
attempt themselves. There are, however,
practical steps you can take to protect your
company from pretexting-related risk. And
you can effectively use technology to
support and manage your pretexting defense.

Following are five core elements of any
pretexting prevention action plan:

Vulnerability assessment
Before taking appropriate measures to
protect your company from pretexting, you
have to first understand your exposures.
Most companies have never looked at
themselves from the outside to determine
who the best targets for pretexting would be
in the eyes of a competitor or saboteur.
Social engineering attempts, after all,
usually don’t target the manager in charge of
sensitive information. Instead, they’re
typically conceived to dupe some
administrative support person. So it takes a
certain degree of familiarity with pretexting
strategies to properly assess an
organization’s vulnerabilities.

Similarly, few companies have adequately
considered which employees are most likely
to be faced with the temptation to pretext as
they seek to fulfill their job requirements.
Even fewer have taken stock of the people
and companies they do business with to
determine which ones, as noted above, pose

a risk as potential pretexting victims or
perpetrators.

Pretexting prevention therefore begins with
a complete assessment of potential
pretexting vulnerabilities. Such an
assessment should include inventories of
both assets requiring protection and the risk-
points associated with those assets – as well
as an evaluation of the potential magnitude
of any associated pretexting event. Based
on this assessment, the protection initiative
can proceed in an informed and well-
focused manner.

Policy definition
You also can’t defend your company against
an enemy you haven’t fully defined. From
an inbound perspective, you need a clear
understanding of how pretexting exploits are
planned and executed. From an outbound
perspective, you have to define in specific
terms what differentiates pretexting from
permissible forms of information gathering.
This definition obviously needs to meet the
standards being set by regulators and
attorneys-general in all relevant
jurisdictions. It must also accurately reflect
your organization’s own ethical standards
and tolerance for risk.

Effective pretexting prevention therefore
requires the creation of well-defined
corporate policies. Such a policy both
defines the objectives of the protection
initiative and plays a central role in its actual
execution. An effective policy will also
transcend individual types of exploits and
address pretexting-related issues in a more
fundamental way.
Communication and training

Once you have a policy in place and you know everyone inside and outside the company who has to understand and comply with that policy, you can start your education process. In addition to helping people recognize a pretexting exploit, such education should teach them what action to take when they find themselves in a questionable situation. That action can be as simple as asking for a name and a number to call back, and then seeking guidance from someone appropriate at the company – since pretexters benefit from immediacy, rather than thoughtful consideration of their requests.

Because time and money probably won’t allow you to make everyone everywhere a subject-matter expert on pretexting, each individual’s education should closely match their particular need. More precisely, specific education “packages” should be designed for and delivered to those in specific roles, departments and/or teams. Because it’s not practical to take people away from their jobs any longer than necessary – or to fill their heads with information they’ll never need or use – every effort should be made to make counter-pretexting education as simple and efficient as possible.

It’s also essential to provide employees and business partners with ready access to appropriate counsel in the event they encounter a situation they’re uncertain about. Such counsel provides a critical resource for front-line staff, who can’t realistically be expected to become policy experts and therefore need a place to turn when they have a question. The availability of counsel – and the fact that everyone has been made aware of and encouraged to use that counsel – is indispensable for effective pretexting defense and for demonstrating counter-pretexting due diligence to regulators.

Certification and documentation

To defend your company from pretexting-related risks – and to effectively transfer risk – you also have to verify that your employees and business partners have actually understood what you’ve trained them on and have agreed to comply with the policies set forth in that training. If you don’t, your training efforts will be of little or no use in a legal or regulatory context.

That’s why it’s essential to document your pretexting-related training activities and have the recipients of that training attest to their understanding of and agreement to your policies. This documentation and compliance attestation must also be appropriately managed so that it can be readily retrieved if and when it becomes necessary to do so.

Change management

Pretexting vulnerabilities change as your business changes. So as you hire and promote employees, engage new partners, bring new information sources online and extend access to existing ones, you have to take appropriate measures. Ideally, the processes by which you’re notified of the need to take such measures should be as immediate and automatic as possible. Otherwise, there’s a good chance it won’t get done.

Whatever system you’re using to manage your counter-pretexting measures should therefore be tightly linked to HR, IT and other relevant areas of the business. That way, your exposure to pretexting-related risks won’t inexorably creep higher over time as a result of business change.
Ideally, of course, pretexting protection should be managed as part of an overall enterprise strategy for governance, risk and compliance. But with so many companies now recognizing the urgency of addressing their most egregious exposures to pretexting risk, it makes sense in the near-term to at least initiate some basic protections using these core elements. Once these immediate steps are taken, counter-pretexting measures can be further expanded and refined as deemed reasonable by management.

The Business Case for Pretexting Prevention

Of course, there are many governance, risk and compliance issues competing for limited corporate resources. Decision-makers therefore need a good reason to invest those resources in pretexting prevention. They also need to know why they should give particular priority to pretexting right now.

The top reasons for getting started immediately with pretexting prevention are:

Rapid, large-magnitude risk reduction
Most companies have already made significant investments in areas such as financial reporting controls and network security. So they have likely already addressed their most egregious vulnerabilities and will probably only reap incremental returns from additional investments in these areas.

On the other hand, few companies have yet taken any real action on pretexting. By taking such action, they are far more likely to discover and remediate major unaddressed vulnerabilities that represent tremendous risk in terms of financial loss, lawsuits, regulatory action, brand damage, and erosion of customer confidence. There is simply more “low-hanging fruit” for most companies in pretexting prevention than in other risk management disciplines that they already have in place.

Significant mitigation of potential consequences
In the unfortunate case that a pretexting incident does occur, it is critically important for a company to have performed – and be able to prove that it has performed – due diligence to prevent such an incident. Such evidence can limit or even prevent regulators and courts from assigning complicity or negligence to corporate executives, and therefore has a significant mitigating impact on the penalties they may choose to impose.

In fact, a credible counter-pretexting initiative is absolutely essential for insulating executives from any failure of its employees, suppliers or business partners to comply with public and corporate policy. Without such an initiative, accountability for any such violation will invariably land in the boardroom.

Timeliness and mindshare
Recent events have made pretexting a top-of-mind issue for both regulators and C-level executives. This makes it important to move on the issue for two reasons. First, regulators are now particularly watchful for this particular brand of corporate misbehavior. So it’s smart to get moving on remediation sooner rather than later.

Second, executives are probably more inclined to endorse such an initiative now than they have ever been before. By acting now, you can capitalize on this window of opportunity and quickly accomplish things
that will benefit the company for years to come. A pretexting initiative can also lay the process and infrastructure groundwork that can be applied to many other important areas of risk and compliance.

**It’s the right thing to do**

Above and beyond any other business benefits, every organization has a fundamental responsibility to promote and ensure the ethical behavior of its members. It’s simply wrong for people to pretend they are someone else in order to achieve financial gain. By taking a stand against pretexting, corporate managers fulfill an obligation to society that falls squarely on their shoulders – and no one else’s.

What do you believe is the right thing to do? Do you have corporate policies in place that explicitly mandate honesty and prudence in all interactions? Do you have effective mechanisms in place for promulgating that policy? Do those mechanisms extend to your suppliers and partners?

If so, you’ll want to make sure you apply those policies and mechanisms appropriately to prevent pretexting from occurring at your company. If not, it’s probably a good idea to take steps now to put them in place. Otherwise, you and your organization will remain vulnerable to the dangers of pretexting.

**About Axentis**

Axentis is the world’s leading provider of on demand enterprise governance, risk and compliance (GRC) management software. Our solutions enable 700,000 users in 100 countries to cost-effectively facilitate and document fulfillment of relevant public and corporate policy mandates. By doing so, these users are able to protect their companies from a broad range of business threats and safeguard their competitive position in today’s highly scrutinized global markets.

Axentis is a particularly attractive business partner for companies seeking to address their pretexting vulnerabilities as quickly and cost-effectively as possible. By leveraging Axentis’ unmatched experience in policy compliance – in conjunction with its on demand tools for managing policy compliance across the enterprise – such companies can readily:

- inventory their pretexting vulnerabilities
- develop appropriate pretexting policies
- comprehensively and appropriately educate and inform all necessary individuals within and beyond the enterprise about those policies
- document all counter-pretexting activities
- streamline ongoing management of counter-pretexting programs

Axentis is headquartered in Cleveland, Ohio with data centers in Boulder, CO and Basel, Switzerland. For more information, please visit [www.axentis.com](http://www.axentis.com) or email APMS@axentis.com.